

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

# THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES

v.

AARON SWARTZ

No. 11-10260-NMG

**MOTION TO SUPPRESS ALL FRUITS OF INTERCEPTIONS AND DISCLOSURES OF  
ELECTRONIC COMMUNICATIONS AND OTHER INFORMATION BY MIT  
PERSONNEL IN VIOLATION OF THE FOURTH AMENDMENT AND THE STORED  
COMMUNICATIONS ACT AND INCORPORATED MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 1)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case (1) the network flow data and DHCP logs collected by MIT personnel and disclosed to the government without a warrant or court order or subpoena, as well as all evidence derived therefrom, and (2) all evidence from the packet capture instituted by MIT personnel on the morning of January 4, 2011, and continuing, at the request of the government that MIT personnel continue to intercept electronic communications, through January 6, 2011, and subsequently turned over to the Secret Service, as well as all evidence derived therefrom.<sup>1</sup>

As reason therefor, defendant states:

<sup>1</sup> In a separate motion to suppress, Swartz contends that after law enforcement agents arrived on the scene on January 4, 2011, and recommended that MIT personnel continue the packet capture they had begun earlier that morning and began to direct the investigation, MIT personnel were acting as government agents, and their actions were therefore subject to the requirements of the Fourth Amendment. See Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law. This motion is directed in part at the interceptions conducted by MIT personnel before they began acting as government agents, as well as MIT's turning over to the government material in which Swartz had a reasonable expectation of privacy, in the complete absence of judicial process compelling MIT to produce such evidence to the government at a time when law enforcement agents were directing MIT employees regarding how to further their criminal investigation of the defendant.

1. He had a reasonable expectation of privacy in the electronic communications flowing to and from his ACER netbook.<sup>2</sup>
2. The interception of network flow data to the netbook and the packet capture constituted interceptions of electronic communications within the meaning of Title III.
3. The interceptions conducted by MIT and its disclosure of the information gathered to the Secret Service violated 18 U.S.C. §2511(1), as no exceptions to the requirements of Title III apply to MIT's conduct. The evidence, along with all derivative fruits thereof, must, therefore, be suppressed as violative of the Fourth Amendment.
4. The disclosure of DHCP logs by MIT personnel in the absence of a warrant issued upon a showing of probable cause or a court order pursuant to 18 U.S.C. §2703(d) violated the Fourth Amendment and/or the Stored Communications Act.
5. MIT's disclosure to the Secret Service of DHCP logs, network flow data, and packet capture information in the absence of a subpoena or search warrant violated 18 U.S.C. §§2702, 2703, as well as Swartz's rights under the Fourth Amendment such that suppression of the evidence, as well as all derivative fruits, is required.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

---

<sup>2</sup> All averments herein regarding Swartz's ownership and possession of the ACER netbook and the attached hard drive, and the communications flowing to and from them, are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).



Network Engineer, which was connected to the netbook and intercepted the communications coming to and from it. *Id.* Later that day, beginning at 11:00 am, the Secret Service assumed control of the investigation.<sup>5</sup> Later on January 4, 2011, Mike Halsall, MIT Senior Network & Information Security Analyst, turned over to Secret Service S/A Michael Pickett "historical network flow data concerning 18.55.6.240 & 7.240 [the IP addresses associated with the earlier JSTOR downloads]<sup>6</sup> dating from 12/14 until present and relevant DHCP log information<sup>7</sup> from prior occurrences of ghost-macbook and ghost-laptop [the two guest registrations at issue] JSTOR downloading incidents (from Sept. and Oct.)." Timeline at 7. The disclosure took place only after the MIT General Counsel's Office approved the disclosure of the information to law enforcement authorities even in the absence of a warrant or court order or subpoena – and at a time when MIT personnel were acting as government agents – and in contravention of MIT policy that such information, which exceeded that found in bank records or telephone toll records, would be disclosed only upon the receipt of lawful court orders or subpoenas, *i.e.*, process complying with the Stored Communications Act, 18 U.S.C. §2701 *et seq.* See Section IV, *infra*. In a separate email from Halsall to S/A Pickett on January 8, 2011, Halsall told Pickett that he "hop[ed] to have the pcap/flows/videos/logs all in by to me Monday,

---

<sup>5</sup> See Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

<sup>6</sup> Network flow data shows connections made between computers and the amount of information transmitted. It shows the start and stop time of a connection, the source IP address, the IP address of the website contacted, source and destination port numbers, and the number of bytes of information transmitted.

<sup>7</sup> "DHCP" stands for Dynamic Host Configuration Protocol. DHCP assists with the assignment of IP addresses to computers on networks. When a computer joins a network, the computer issues a DHCP request on the network, which asks a DHCP server on the network to provide an IP address to the requesting computer. Part of the information contained in this request is the MAC (Media Access Control) address which is a unique identifier of the network card contained in the computer requesting an IP address. It also includes the commands made by the computer in question. See page 7, *infra*.



possibly sooner – if you don't already have a copy of the video or pcap [packet capture], I'll make sure you get one." Exhibit 2. No warrant or court order has been provided to counsel which would evidence the government's having, even post-interception, acquired the contents of the warrantless interceptions by seeking judicial authorization as required.

## **II. MIT'S ACTIONS VIOLATED TITLE III.**

### **A. Swartz Had a Reasonable Expectation of Privacy in his Electronic Communications to and from his Netbook.<sup>8</sup>**

Swartz had a subjective expectation of privacy in electronic communications to and from his netbook, and that expectation is one which society should recognize as objectively reasonable. The netbook was connected to the MIT network, but "the mere act of accessing a network does not in itself extinguish privacy expectations," *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). MIT has a liberal guest access policy, which was described by Tim McGovern, MIT Manager of Network Security & Support Services, as follows:

No authentication of visitors. Visitor network access is provided as an on-demand self-service process for anyone who walks onto campus, plugs in, or elects to use our wireless network, and declares themselves a visitor, and they get 14 days of network privileges.

No identity verification. Visitors are asked to provide an email address. The email address is not used to verify that a bona fide identity exists . . . .

No authentication of users accessing JSTOR.org. By agreement, JSTOR.org allows any computer with a net 18 IP address [an MIT IP address] to access their resources without further identification or authentication.

Exhibit 3. In fact, in internal emails, JSTOR described MIT as "unique" in having an open campus.

Exhibit 4. Unlike other institutions which require passwords to access their servers and require additional layers of authentication to access digital libraries such as JSTOR, MIT required neither

---

<sup>8</sup> Swartz incorporates by reference the discussion in Section II of his Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

The DHCP server is in a secure location and complies with secure data storage best practices. IS&T's Network Services Infrastructure team acts as the data custodian for DHCP logs, and ensures that the logs are stored securely and are deleted when they expire.

\* \* \* \*

*MIT is required to comply with a court order or valid subpoena that requests the disclosure of information contained in DHCP logs. Failure to comply could have serious consequences for the individuals, IS&T, and the Institute. MIT's Office of the General Counsel is qualified and authorized to confirm that a request for information contained in logs is legitimate and not an improper attempt to gain access to confidential information.*

*Id.* (emphasis added).

Moreover, on many occasions, the MIT RADIUS log server provided further evidence documenting MIT's authorization of Swartz's access to the MIT network:

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. . . . Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. . . . The RADIUS server is usually a background process running on a UNIX or Microsoft Windows server. RADIUS serves three functions:

- to authenticate users or devices before granting them access to a network,
- to authorize those users or devices for certain network services and
- to account for usage of those services.

<http://en.wikipedia.org/wiki/RADIUS> (last visited September 23, 2012)(emphasis added). Swartz, accordingly, maintained a reasonable expectation of privacy in the communications to and from his netbook and that expectation was objectively reasonable.

**B. MIT's Actions in Intercepting Communications to and from Swartz's Netbook and Disclosure of the Intercepted Communications Violated Title III.**

18 U.S.C. §2511(1) prohibits:

(a) intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

\* \* \* \*

(e) intentionally disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the

information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally us[ing], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . .

18 U.S.C. §2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce . . . ." Section 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." "Contents" is in turn defined as "any information concerning the substance, purport or meaning" of the communication. §2510(8)(emphasis added).

The packet capture, which targeted the content of data being sent to or from the netbook that was discovered in Building 16's data room, revealed the contents of electronic communications of all electronic communications intercepted. See Email from Dave Newman, MIT Senior Network Engineer, to S/A Pickett, January 5, 2011, Exhibit 12 ("I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads"). Use of the packet capture constituted the interception of electronic communications of the defendant and others, including, but not limited to, those with whom he was communicating within the meaning of Title III, *see, e.g., United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*)(diverting incoming communications constitutes interception within the meaning of Title III), which was unlawful in the absence of a valid Title III order authorizing the interceptions of the electronic communications, of which none were sought or issued here.

The DHCP logs also captured content as they captured the message sent from the sending computer requesting an IP address, which is the “substance, purport, or meaning” of the communication.<sup>9</sup> The network flow data showed that a communication took place between one computer and another and the amount of information transmitted. These, too, constitute “contents.”<sup>10</sup> In *In re Application of United States*, 396 F.Supp.2d 45, 48-49 (D.Mass. 2005), the Court recognized that “dialing, routing, addressing and signaling information” may disclose “content” and mandated that the order include instructions to the provider that “[t]he disclosure of the ‘contents’ of communications is prohibited pursuant to this Order even if what is disclosed is also dialing, routing, addressing and signaling information” and that “the term ‘contents’ of communications includes subject lines, application commands, search queries, requested file names, and file paths.” See, e.g., *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) (suggesting that a technique which reveals the URL visited would be “constitutionally problematic”).

Therefore, the interceptions were unlawful unless they fell within an exception to the prohibitions of §2511. The “provider exception” to Title III, §2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a *necessary incident to the rendition of his service or to the protection of the rights and property of the provider of that service* . . . .

---

<sup>9</sup> Another issue specific to the DHCP logs is addressed in Section III, *infra*.

<sup>10</sup> Such information is not analogous to a pen register, which has been held not to reveal content, because a pen register does not even show whether a communication even took place, see *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977). Even a pen register requires a court order based upon a “certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.” 18 U.S.C. §3122(b)(2).

(emphasis added).<sup>11</sup> "The statute's use of the word necessary, its proviso restricting random monitoring and Congress' intent to maximize the protection of privacy . . . suggests that this authorization should be limited in scope." *United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975). See, e.g., *United States v. Cornfeld*, 563 F.2d 967, 970 (9th Cir. 1977) ("the authority to intercept and disclose . . . communications is not unlimited"); *United States v. Harvey*, 540 F.2d 1345, 1350 (8th Cir. 1976) (authority granted by §2511(2)(a)(i) "may be exercised only to the extent necessary for 'the protection of the rights and property of the carrier'"); *United States v. McLaren*, 957 F.Supp. 215, 218 (M.D.Fla. 1997) ("the court must consider whether the provider of electronic communication service had reasonable cause to suspect that *its* property rights were being abused by a particular subscriber" (emphasis added)).

Here, the circumstances demonstrate that MIT personnel did not intercept the communications at issue to protect *MIT's* rights or property as a provider of electronic communication service. Instead, its concern was initially with the protection of the rights and property of JSTOR and thereafter with assisting law enforcement with discovering the motive and intent of the owner of the netbook and in acquiring evidence that would further the criminal investigation of the individual responsible for the JSTOR downloading. Once the netbook was physically discovered, MIT personnel, aware that its owner would return to retrieve the external hard drive that was attached to the netbook and receiving the downloaded data, installed video surveillance to identify the owner and help in his apprehension. The investigation commenced with a notification from JSTOR regarding excessive downloads of journal articles, and thereafter MIT

---

<sup>11</sup> 18 U.S.C. §2510(15) defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications."

personnel worked with JSTOR to develop and institute a plan which would prevent MIT guest users from accessing JSTOR without an additional level of authorization and permission. There was no need for further investigation on MIT's part, as its electronic communication system was never in the slightest danger of injury or other detrimental impact. Once the netbook was located, MIT advised JSTOR of the discovery and asked it to block the particular IP address it was using. See Exhibit 13. MIT also had the option, which it did not choose to exercise, to simply take the netbook offline. Instead, it kept the connection alive only to assist law enforcement and to further a criminal investigation, objectives well outside the narrow parameters of the provider exception to the general prohibition of warrantless interceptions of wireless communications in transit.

Even at the outset of the investigation which began again on January 3, 2011, the objective was to placate JSTOR, which had deemed MIT's prior efforts to identify the person responsible for the downloads "tepid," Exhibit 14, and ensure continued MIT access to JSTOR, as witness the central role played in the investigation by Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, and not a "necessary incident" to the "protection of the rights and property" of MIT as electronic communications service provider. As of the next morning, January 4, 2011, MIT personnel were acting as agents of law enforcement, and their purpose was not to protect MIT's electronic communications system but instead to further the criminal investigation.<sup>12</sup> Section 2511(2)(a)(i) does not extend to the protection of institutional interests in general but instead only to the protection of the electronic communication system itself.<sup>13</sup> Once the ACER was located

---

<sup>12</sup> See Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

<sup>13</sup> The interceptions also did not fall within the "trespasser exception," §2511(2)(i), because Swartz was not a trespasser, see Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law at 16-19, and, most importantly for present purposes, MIT personnel were not, until law enforcement agents

on the morning of January 4, 2011, MIT's problem with JSTOR could have been ended by disconnecting that computer from the MIT network. Instead, it elected to intercept communications, not to protect the MIT system, but to gather information for law enforcement purposes, such as the motive and intent of the person responsible for the downloads, and to determine whether any of the downloaded information had been transmitted to others by the netbook, a purpose which was protective of JSTOR and in furtherance of law enforcement's acquisition of proof of the possible commission of various federal offenses, but not protective of MIT's electronic communication services, as required by the statutory exception.

Moreover, even if the Court were to conclude that MIT, as electronic communications service provider, was acting to protect its own interest *qua* service provider as it searched for the "offending" computer, "the federal courts . . . have construed [§2511(2)(a)(i)] to impose a standard of reasonableness upon the investigating communication carrier." *United States v. Harvey*, 540 F.2d 1345, 1351 (8th Cir. 1976). *See, e.g., United States v. Hudson*, 2011 WL 4727811 at \*7 -\*8 (E.D.La. Oct. 5, 2011) ("The Fifth Circuit has held that this provision imposes a reasonableness requirement on carriers," citing *United States v. Clegg*, 509 F.2d 605, 613-14 (5th Cir. 1975)); *United States v. McLaren*, 957 F.Supp. 215, 218 (M.D.Fla. 1997) (court "must consider whether the interception activities were reasonable"). The interceptions at issue here went far beyond anything that was necessary to the protection of MIT's rights and property; prior to the January 4, 2011, interceptions and the warrantless disclosures of protected information, the ACER laptop had been discovered, its connection to the MIT network had been identified, video surveillance had been instituted to identify the owner, and a narrow shutdown of service to that computer would have accomplished any legitimate goal of protecting MIT's electronic communication service.

---

encouraged and adopted the ongoing packet capture, acting "under color of law."

Similarly, an electronic communications system provider may disclose to law enforcement *only* those intercepted communications which are a “necessary incident” to the protection of the provider’s property rights. *See, e.g., Clegg*, 509 F.2d at 612-13. *See, e.g., United States v. Auler*, 539 F.2d 642, 646 n.10 (7th Cir. 1976) (“Evidence which is obtained through an unreasonably broad surveillance cannot be legally disclosed to the government, regardless of whether it is offered at trial”). Only those communications of which §2511(2)(a)(i) reasonably permits the interception may be disclosed and admitted as evidence at the trial of a criminal case; “evidence obtained through surveillance beyond the authorization of §2511(2)(a)(i) . . . must be suppressed.” *Id.* at 646. None of the disclosures on January 4, 2011, was justified by this narrow exception to an MIT guest’s entitlement to the protections of the Fourth Amendment and Title III. As such, consistent with *Councilman*, the network data capture constituted unlawful interceptions of electronic communications in violation of the Fourth Amendment, requiring suppression of the captured information and all evidence derived therefrom.

**III. THE GOVERNMENT COULD NOT OBTAIN DHCP LOG INFORMATION IN THE ABSENCE OF A WARRANT OR, AT MINIMUM, A §2703(D) ORDER.**

The DHCP log records and stores a variety of data. *See* page 7, *supra*. For present purposes, the critical fact about DHCP addressees is that their recording and storage allows the tracking of an individual through the location of his computer. Where laptops and other portable devices are concerned, that data is comparable to cell site data in that it permits the government to determine an individual’s location and to track his movements as he moves his laptop from place to place. Two types of DHCP data are at issue here: the historical data which the government sought from MIT, and with which MIT provided the government, and the ongoing real-time DHCP data which law enforcement obtained on an ongoing basis after they assumed control of the investigation on January



4, 2011, all of which was sought, and obtained, by the government without a warrant or a court order issued pursuant to §2703(d).

Individuals have a reasonable expectation of privacy in their movements. *See, e.g., In re Application of United States*, 849 F.Supp.2d 526, 538-43 (D.Md. 2011). Moreover, an individual retains a reasonable expectation of privacy in DHCP log information because, as the Third Circuit held in the cell site location context, “a . . . customer has not ‘voluntarily’ shared his information with [a third party] in any meaningful way.” *In re Application of United States*, 620 F.3d 304, 317 (3d Cir. 2010). As Justice Sotomayor explained in her concurring opinion in *United States v. Jones*, 132 S.Ct. 945 (2012):

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith [v. Maryland]*, 442 U.S. [735,] 742 [(1979)] . . . ; *United States v. Miller*, 425 U.S. 435, 443 . . . (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice ALITO notes, some people may find the “tradeoff” of privacy for convenience “worthwhile,” or come to accept this “diminution of privacy” as “inevitable,” . . . and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. *See Smith*, 442 U.S., at 749 (Marshall, J., dissenting) (“Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes”); see also *Katz [v. United States]*, 389 U.S. [347,] 351-352 [(1967)] (“[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected”).

*Id.* at 957.

As to both historical and "real time" cell site data, courts have been divided regarding whether the government must demonstrate probable cause as required by the Fourth Amendment or whether the lesser showing required under §2703(d) will suffice. Compare *In re Application of the United States*, 2012 WL 3260215 at \*1-\*2 (S.D.Tex. July 30, 2012); *In re Application of the United States*, 809 F.Supp.2d 113, 118-20 (E.D.N.Y.2011); *In re United States*, 747 F.Supp.2d 827, 837-40 (S.D.Tex.2010); *In re Application of United States*, 736 F.Supp.2d 578, 579 (E.D.N.Y.2010)(requiring showing of probable cause), with *In re Application of United States*, 620 F.3d at 313; *In re Application of United States*, 849 F.Supp.2d 177, 179 (D.Mass. 2012); *United States v. Graham*, 846 F.Supp.2d 384, 396 (D.Md. 2012); *United States v. Benford*, 2010 WL 1266507, at \*2-\*3 (N.D.Ind. March 26, 2010); *In re Applications of United States*, 509 F.Supp.2d 76, 80-81 (D.Mass. 2007); *In re Application of United States*, 396 F.Supp.2d 294, 327 (E.D.N.Y. 2005)(§2703(d) order suffices).

Courts are likewise split with respect to the government's burden to obtain real time cell site data. Compare *In re Application of the United States*, 849 F.Supp.2d 526 (D.Md. 2011); *In re Application of the United States*, 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009); *In re Application of the United States*, 497 F.Supp.2d 301 (D.P.R.2007); *In re Application of the United States*, 2006 WL 2871743 (E.D.Wis. Oct. 6, 2006); *In re Application*, 439 F.Supp.2d 456 (D.Md.2006); *In re United States*, 441 F.Supp.2d 816 (S.D.Tex.2006); *In re United States*, 2006 WL 1876847 (N.D.Ind. July 5, 2006); *In re Application of the United States*, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006); *In re United States*, 416 F.Supp.2d 390 (D.Md.2006); *In re United States*, 415 F.Supp.2d 211 (W.D.N.Y.2006); *In re United States*, 412 F.Supp.2d 947 (E.D.Wis.2006), *aff'd* 2006 WL 2871743 (E.D.Wis. Oct. 6, 2006); *In re United States*, 407 F.Supp.2d 134 (D.D.C.2006)(requiring a showing of probable cause), with *In re Application of the United States*, 2008 WL 5255815 (E.D.N.Y.

Dec.16, 2008); *In re United States*, 2008 WL 5082506 (E.D.N.Y. Nov. 26, 2008); *In re Application of the United States*, 460 F.Supp.2d 448 (S.D.N.Y.2006); *In re United States*, 433 F.Supp.2d 804 (S.D.Tex.2006); *In re Application of the United States*, 415 F.Supp.2d 663 (S.D.W.Va.2006); *In re Application of the United States*, 411 F.Supp.2d 678 (W.D.La.2006)(probable cause not required).

The cases requiring a showing of probable cause for both historical cell site data and real time cell site data are the better reasoned and more consonant with the requirements of the Fourth Amendment and its historical role in protecting citizens from serious invasions of personal privacy. The same analysis is applicable to both historical DHCP data and real time DHCP data, and the government's acquisition of this information in the absence of a warrant based on probable cause violated the Fourth Amendment. The invasion of this information also has serious First Amendment implications in that it traces an individual's communicational associations. *See In re Application of United States*, 849 F.Supp.2d at 538 n.5. At a minimum, a §2703(d) order was required. Accordingly, the DHCP log information, and all information derived therefrom, including the laptop and hard drive seized from the MIT Student Center which were discovered as an unattenuated result of the "real time" inspection of DHCP logs on January 6, 2011, must be suppressed.

#### **IV. MIT'S ACTIONS VIOLATED THE STORED COMMUNICATIONS ACT ("SCA").**

18 U.S.C. §2702(a)(1) prohibits any person or entity "providing an electronic communication service to the public" from "knowingly divul[ging] to any person or entity the contents of a communication while in electronic storage by that service."<sup>14</sup> Section 2702(a)(3) prohibits "a provider of . . . electronic communication service to the public" from "divulg[ing] a record or other

---

<sup>14</sup> "Electronic storage" includes "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic service communication provider for purposes of backup protection of such communication." 18 U.S.C. §2510(17).

information pertaining to a subscriber or a customer of such service . . . .” MIT was a provider of electronic communication service to the public because it freely allowed guests with no affiliation to MIT to access the MIT network and because it provided wireless service which was readily accessible to anyone within reach of its signal, which extended to areas outside the bounds of the MIT campus.<sup>15</sup> As a guest, Swartz was a customer or subscriber of MIT’s electronic communication service. The SCA contains a provider exception similar to that of Title III: the provider of electronic communication service may disclose the content of communications or information pertaining to a subscriber or customer “as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service.” §§2702(b)(5), (c)(3). This exception does not apply for the same reasons previously addressed in conjunction with the provider exception of Title III.

Moreover, here, MIT did not voluntarily disclose the information on its own initiative. Indeed, disclosure of the information was contrary to MIT policy, which provided its users, including guests, with a reasonable expectation of privacy in the DHCP logs and other information collected by MIT. *See* pages 7-8, *supra*. MIT disclosed the information only after its General Counsel’s office authorized the disclosure, *which had been requested by the government after it had assumed control of the investigation and after MIT had deferred to the government’s control over the investigation*. Thus, at the time of the disclosures, MIT personnel were acting as government agents. In short, MIT personnel, by the late morning of January 4, 2011, were acting as agents of federal and state law enforcement.

Congress passed the Stored Communications Act in 1986 as part of the Electronic Communications Privacy Act. “The SCA was enacted because the advent of the Internet

---

<sup>15</sup> MIT’s wireless network signal is available outside of the campus, for example, at the Kendall Hotel and on the streets and sidewalks that border the campus.

presented a host of potential privacy breaches that the Fourth Amendment does not address." *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir.2008)[, *rev'd on other grounds sub nom. City of Ontario v. Quon*, 130 S.Ct 1531 (2010)] (citing Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1209-13 (2004)). The SCA prevents "providers" of communication services from divulging private communications to certain entities and individuals. Kerr, *supra*, at 1213. It "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." *Id.* at 1212. First, the statute limits the government's right to compel providers to disclose information in their possession about their customers and subscribers. 18 U.S.C. § 2703. . . . Second, the statute limits the right of an Internet Service Provider ("ISP") to disclose information about customers and subscribers to the government voluntarily. 18 U.S.C. § 2702.

*Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965, 971-72 (C.D. Cal. 2010).

As addressed in the previous section, MIT could not voluntarily disclose the information without violating the SCA. Under §2703, the government could not lawfully request or obtain access to the content of electronic communications in the absence of a warrant issued in accordance with the Rules of Criminal Procedure. 18 U.S.C. §2703(a).

In passing the Electronic Communications Privacy Act in 1986, Congress expressed the need to expand the protections of the Fourth Amendment to new forms of communication and data storage. 132 Cong. Rec. H4039-01 (1986); S.Rep. No. 99-541, at 1-2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-56. The legislative history indicates that Congress wished to encourage the development and use of these new methods of communication by ensuring that they were protected and private. S.Rep. No. 99-541, at 5. Congress recognized that courts had struggled with the application of the Fourth Amendment to the seizure of intangibles, like telephone conversations. *Id.* at 2. They therefore sought to strike a balance between the competing interests addressed by the Fourth Amendment in the world of electronic communications by "protect[ing] privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." *Id.* at 3.

It is clear that Congress wished to apply the protections associated with search warrants to searches authorized under § 2703(a).

*In re United States*, 665 F.Supp.2d 1210, 1220 (D.Or. 2009). The government could not lawfully obtain "record[s] or other information pertaining to a subscriber or customer" of MIT's electronic communications system in the absence of a warrant or a court order issued pursuant to §2703(d). 18 U.S.C. §2703(c)(1). Under §2703(c)(2), the government may obtain the name and address of a

customer or subscriber, records of session times and duration, length of services and types of service used, and "other subscriber number or identity, including any temporarily assigned network address" only through an administrative, grand jury, or trial subpoena. The information at issue here went beyond this narrow description, but, in any event, the government did not seek the information pursuant to subpoena. The DHCP logs, the network flow data, and the packet capture all either contained "content" of the electronic communications to and from the netbook, in which Swartz had a reasonable expectation of privacy or "record[s] or other information" pertaining to Swartz's use of MIT's electronic communications system, in which he also had a reasonable expectation of privacy. Indeed, MIT's DHCP log policy created an objectively reasonable expectation that those logs would remain confidential unless they were required to be disclosed pursuant to a lawful order or subpoena, of which there was none here. The government's conduct, in seeking the production of this material without a warrant and without a §2703(d) order violated the Fourth Amendment. *See, e.g., United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The material at issue must, accordingly, be suppressed, along with all derivative fruits thereof.

Respectfully submitted,  
By his attorney,

/s/ Martin G. Weinberg  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owimgw@att.net

**CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to the motion was served on the government by hand this same date.

/s/ Martin G. Weinberg

Martin G. Weinberg

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

AARON SWARTZ,

Defendant

)  
)  
) Criminal No. 11-10260-NMG  
)  
)  
)

**GOVERNMENT'S CONSOLIDATED RESPONSE TO  
DEFENDANT'S MOTIONS TO SUPPRESS**

The Court should deny Defendant Aaron Swartz's five motions to suppress (Dkt. Nos 59-63), which attack the manner in which the Government collected the vast majority of electronic and physical evidence in this case.

**I. INTRODUCTION**

**A. The Victims: JSTOR and MIT**

A research or university library can find the cost and space to maintain a comprehensive collection of academic journals extraordinarily expensive. Founded in 1995, JSTOR is an independent, self-sustaining, non-profit organization that provides research and university libraries access to numerous academic journals without the normal costs of a paper-based collection. To do so, JSTOR digitizes articles and distributes them over an online system that it built, which enables libraries to outsource the journals' storage, ensures their preservation, and enables them to be searched extensively by authorized users.

JSTOR pays copyright-holders for permission to digitize the copyright-holders' articles and make them available online.<sup>1</sup> To pay its expenses, JSTOR normally charges subscription

---

<sup>1</sup> Some materials available on JSTOR are not subject to copyright.



fees to its customers. For this access, a large research library might pay JSTOR more than \$50,000 a year. In addition, JSTOR also charges customers for access to certain individual journal articles on an article-by-article fee. JSTOR shares portions of its fees with the articles' and journals' copyright-holders.

As at any library, users of JSTOR are to access articles a few at a time as they need them for their research. JSTOR employs computerized methods to track and limit its users' downloading activity. In addition to these computerized methods, before a legitimate user can download an article from JSTOR, the user is prompted to review and accept JSTOR's terms of service. (Ex. 1). Each article downloaded from JSTOR also comes with a cover page confirming the user's acceptance of the terms of service and a link to the location where the terms are found. (Ex. 2). The terms of service, commonsensibly, state that you cannot use automated computer programs to systematically download and export content from JSTOR's archive. (Ex. 3). The user prompt, cover sheet, and terms of service emphasize that you cannot download an entire issue of a journal without prior permission. (Exs. 1-3).

The Massachusetts Institute of Technology ("MIT") is a renowned scientific research university. When a guest registers his computer on MIT's computer network, he must agree to follow the same computer rules of use that the faculty, students and employees must follow. These rules of use require that the guest's activities on MIT's network be consistent with the network's purpose of supporting research, education and MIT administrative activities. In return, MIT assigns the guest an IP address<sup>2</sup> and allows the guest computer network service for a

---

<sup>2</sup>An IP (Internet protocol) address is like a telephone number for a computer. Each computer attached to the Internet must be assigned an IP address so the computer's incoming and outgoing Internet traffic can be directed properly from the traffic's source to its destination. An

short period, only 14 days per year. (Ex. 4). As configured during the events alleged in the Superseding Indictment, a guest whom MIT had granted an IP address could request and receive digitized journal articles from JSTOR.

**B. The Defendant: Aaron Swartz**

During the period alleged in the Superseding Indictment, Aaron Swartz was a fellow at Harvard University's Safra Center for Ethics, on whose website he was described as a "writer, hacker and activist." Harvard provided Swartz with access to JSTOR's services and archives as needed for his research there. Swartz was not a student, faculty member, or employee of MIT. In the Guerilla Open Access Manifesto, which Swartz actively participated in drafting and had posted on one of his websites, Swartz advocated "tak[ing] information, wherever it is stored, mak[ing] our copies and shar[ing] them with the world." (Ex. 5).

**C. Overview of the Offenses**

Between September 24, 2010 and January 6, 2011, Swartz schemed to (a) break into a restricted-access network wiring closet at MIT; (b) attach his computer to a network switch within that closet and thus access MIT's computer network; (c) use MIT's computer network to access JSTOR's archive of digitized journal articles; (d) download a substantial portion of JSTOR's archive onto his computer and computer hard drives, which at times impaired the operation of JSTOR's computers and resulted in MIT's loss of JSTOR access; (e) avoid MIT's and JSTOR's efforts to prevent this type of massive copying, efforts that were directed at users

---

IP address consists of a unique series of four numbers, each ranging from 0-225, separated by periods (e.g., 18.55.7.216). For example, when a user types in the District Court's website address as "www.mad.uscourts.gov", his computer network translates that phrase into the website hosting computer's IP address, 199.107.17.221, to direct his communications to the site.

generally and at Swartz specifically; and (f) elude detection and identification.

## II. THE FACTS

Late during the night of September 24, 2010, an individual registered his computer on MIT's campus and obtained a guest account on MIT's computer network. The individual did not provide his true identity at this or any subsequent time, and neither MIT personnel nor law enforcement officers knew the individual's name until his arrest months later. The individual registered his computer by specifying his name as "Gary Host," a pseudonym, and his e-mail address as ghost@mailinator.com, a disposable e-mail address by virtue of its requiring no initial e-mail registration and keeping no records of e-mail access.<sup>3</sup> Before assigning the computer an IP address, MIT's network automatically collected the computer's owner-created name — "ghost laptop" — and the unique identifying number associated with the computer's Internet networking hardware, known as the computer's Media Access Control or "MAC" address. These are standard login and communication procedures.

MIT's DHCP<sup>4</sup> computer server then used a standard Internet protocol to assign the individual an IP address (18.55.6.215) for use while on the network. The network kept records of the computer's registration information, its IP address, and its MAC address. These records are standard computer-networking records, and did not include any computer commands that the individual typed in or ran, or any data that the computer downloaded. (Exs. 6, 7).

---

<sup>3</sup> Mailinator advertised itself as a free e-mail service that would accept mail for any e-mail address directed to mailinator.com without need for a prior registration or account; would automatically delete all e-mail after several hours, whether read or not; and would keep no logs (records) of e-mail access.

<sup>4</sup> DHCP is the acronym for Dynamic Host Configuration Protocol.

On September 25, 2010, the day after registering the "ghost laptop," the individual used the "ghost laptop" to systematically access and rapidly download an extraordinary volume of articles from JSTOR by using a software program that sidestepped JSTOR's computerized limits on the volume of each user's downloads. The downloads and requests for downloads were so numerous, rapid, and massive that they impaired the performance of JSTOR's computers.

As JSTOR, and then MIT, became aware of these downloads and problems, both attempted to block the individual's computer from further communications. On the evening of September 25, 2010, after suffering hundreds of thousands of downloads from the ghost laptop, JSTOR temporarily ended the downloads by blocking network access from the computer at IP address 18.55.6.215.

The next day, however, the ghost laptop's user obtained a new IP address from MIT's network, changing the last digit in its IP address by one from 18.55.6.21~~5~~ to 18.55.6.21~~6~~. This defeated JSTOR's IP address block, enabling the ghost laptop to resume furiously downloading articles from JSTOR. This downloading continued until the middle of September 26, when JSTOR spotted it and blocked communication from IP address 18.55.6.216 as well.

The September 25 and 26 downloads had impaired JSTOR's computers and misappropriated significant portions of its archive. Because the download requests had originated from two MIT IP addresses that had begun with 18.55.6 — that is, 18.55.6.215 and 18.55.6.216 — JSTOR began blocking a broader range of MIT IP addresses on September 26. The new block prevented MIT researchers assigned MIT IP addresses 18.55.6.0 through 18.55.6.255 (as many as 253 computers) from performing research through JSTOR's archive for three to four days.

Moreover, when JSTOR notified MIT of the problems, MIT, too, banned the "ghost laptop" from using its network. To do this, MIT terminated the ghost laptop's guest registration on September 27, 2010, and prohibited the computer, as identified by its hardware MAC address, from being assigned a new IP address again through the guest registration process.

On October 2, 2010, less than a week after JSTOR and MIT had barred the individual's ghost laptop from communicating with their networks, the individual obtained yet another guest connection for the ghost laptop on MIT's network. Having recognized that MIT or JSTOR had blocked his ghost laptop by recognizing its MAC address, the individual now manipulated the ghost laptop's MAC address to mislead MIT into believing that he was a new and different guest registrant.<sup>5</sup>

Six days later, the individual connected a second computer to MIT's network and created another guest account using pseudonyms similar to those he had used with the "ghost laptop": he registered the new computer under the name "Grace Host", a temporary email address of ghost42@mailinator.com, and a computer client name of "ghost macbook."

On October 9, 2010, the individual activated the ghost laptop and the ghost macbook to download JSTOR's articles once again. The downloads came so fast and numerous that the individual again significantly impaired the operation of some of JSTOR's computers.

Once again, MIT could not identify who was controlling these computers or where they were physically located, and JSTOR could not isolate the interloper to a consistent IP address

---

<sup>5</sup> A computer's MAC address is initially assigned by an equipment manufacturer, but can be misrepresented electronically by a knowledgeable user. The user altered the ghost laptop's MAC address to appear as 00:23:5a:73:5f:fc rather than the prior MAC address of 00:23:5a:73:5f:fd.

that could be blocked. Consequently, JSTOR blocked access by *every* computer using an MIT IP address campus-wide for approximately three days, again depriving legitimate MIT users from accessing JSTOR's services. And MIT blocked computers using the ghost laptop's and the ghost macbook's MAC addresses as well.

Nevertheless, between the end of October and January 6, 2011, the hacker obtained at least three new IP addresses and assigned his computer two new MAC addresses. He also moderated the speed of the downloads, which made them less noticeable to JSTOR. The exfiltration of JSTOR's collection was nonetheless extreme: over this period, the individual downloaded well over a million of JSTOR's articles.

Because the hacker had modified the speed of his downloads, JSTOR did not notice his latest downloads until around Christmas, 2010. Once noticed, however, JSTOR provided MIT with the hacker's latest IP address. Now that MIT's network security personnel had a more robust set of network tools, they could consult network traffic routing records and trace the IP address back to a concrete physical location on campus.

So on January 4, 2011, an MIT network security analyst traced the hacker's IP address to a network switch located in a basement wiring closet in MIT's Building 16. Building 16's street-level doors have no-trespassing signs posted on them. (Ex. 8). The wiring closet is protected by a pair of locked steel doors. (Ex. 9). The closet is generally locked, but at that time its lock could be forced by a quick jerk of its double doors. When MIT personnel entered the closet, they found a cardboard box with a wire leading from it to a computer network switch. (Ex. 10).<sup>6</sup>

---

<sup>6</sup> MIT personnel removed the box from the laptop at first, and then MIT personnel or law enforcement officers replaced the box on one or more occasions. The second photograph was taken after the box was replaced, not when it was initially found.

Hidden under the box was the ghost laptop, an Acer-brand laptop, connected to a separate hard drive for excess storage. (Ex. 11). The network cable connected the laptop to the network switch, thus giving the laptop Internet access. (Ex. 12). The laptop's direct connection to the network switch was unusual because MIT does not connect computers directly to those switches.

MIT called campus police to the scene, who, in turn, brought in the Cambridge Police and the Secret Service. Over the course of the morning and early afternoon of January 4th, MIT and law enforcement officers collaboratively<sup>7</sup> took several steps to identify the perpetrator and learn what he was up to:

- (1) Cambridge Police crime scene specialists fingerprinted the laptop's interior and exterior and the external hard drive and its enclosure;
- (2) MIT placed and operated a video camera inside the closet, which, as discussed below, later recorded the hacker (subsequently identified as Aaron Swartz) entering the wiring closet and performing tasks within it;
- (3) The Secret Service opened the laptop and sought to make a copy of its volatile memory (RAM), which would automatically be destroyed when the laptop's power was turned off, but the effort resulted in their seeing only the laptop's user sign-in screen;
- (4) MIT connected a second laptop to the network switch in order to record the laptop's communications, a type of recording often referred to as a "packet capture;" the Secret Service subsequently concurred with the packet capture, none of which was turned over to officers until MIT was issued a subpoena after Swartz's arrest;<sup>8</sup>
- (5) Beginning on January 4, 2011, MIT agreed to provide, and later provided, the Secret Service copies of network logs pertaining to

---

<sup>7</sup> From the time of law enforcement's arrival on January 4, 2011, through the suspect's arrest and identification on January 6, 2011, the effort by MIT and law enforcement to identify the individual was both consensual and collaborative.

<sup>8</sup> This second laptop is seen on a chair in Ex. 10.

the ghost laptop and ghost macbook between September 24, 2010 and January 6, 2011, some of which records were provided consensually, the remainder of which were provided pursuant to a subpoena to MIT.<sup>9</sup>

By mid-day on January 4th, MIT and law enforcement personnel had completed their initial crime scene investigation. Experience told them that merely removing the hacker's computer equipment would just result in his renewing his efforts elsewhere. So, rather than take the hacker's equipment away, MIT and law enforcement instead restored the closet to its initial appearance upon discovery, and monitored who entered it and handled the laptop. In this way, the hacker would not necessarily know that his criminal tools had been discovered, his identity might be uncovered, and he could be stopped.

The ruse worked. Within an hour of their departure, the hacker returned. After entering the wiring closet and shutting the doors behind him, (Ex. 13), the hacker replaced the hard drive connected to the laptop with a new one he took from his backpack, and then concealed his equipment once again underneath the cardboard box.

Two days later, on January 6, 2011, the hacker returned to the wiring closet yet again. This time, worried about being identified, the hacker covered his face with his bicycle helmet as he entered the closet. (Ex. 14). Once inside and with the door closed, the hacker disconnected the laptop and placed it, the external hard drive, and the network cable in his backpack. (Ex. 15). As he left, he again hid his face with his bicycle helmet. (Ex. 16).

By January 6, 2011, the hacker had downloaded a major portion of the 6 to 7 million articles then contained in JSTOR's digitized database.

---

<sup>9</sup> As discussed below, both the law and MIT's policies and procedures allowed MIT to turn these records over consensually, but it also could, and at points did, insist upon a subpoena.



A little after 2:00 that afternoon, MIT Police Captain Albert Pierce, who had been involved in the investigation, was heading down Massachusetts Avenue within a mile of MIT when he spotted a bicyclist who looked like the hacker caught on the wiring closet video. Captain Pierce identified himself as a police officer. After a brief exchange, the individual dropped his bike to the ground and ran away. The individual was chased, apprehended, arrested, and identified as Aaron Swartz. During a search incident to arrest, Cambridge police found a USB storage drive in Swartz's backpack, which they seized and stored as evidence.

Approximately an hour later, MIT technical staff used computer routing and addressing records to locate Swartz's ghost laptop and hard drive in the Student Information Processing Board's office in MIT's student center. Law enforcement found the equipment on the floor under a desk. (Ex. 17). The equipment was subsequently seized and stored as evidence by Cambridge Police.

Aaron Swartz was charged by the Commonwealth in a criminal complaint alleging breaking and entering into MIT's property with intent to commit a felony, and was subsequently indicted by a Massachusetts grand jury for the same charge along with stealing JSTOR's electronically processed or stored data, and accessing a computer system without authorization.

While the Commonwealth pursued state charges, the U.S. Attorney's Office began a separate investigation on January 5, 2011. On February 9, 2011, the Secret Service obtained a warrant to search Swartz's apartment, followed by a warrant to search his office on February 11, 2011. Both were executed on February 11th. Also on February 9, 2011, the Secret Service obtained warrants to seize from the Cambridge Police and then search the laptop, the hard drive, and the USB storage device. These warrants were returned unexecuted and new warrants were

obtained on February 24, 2011. On May 16, 2011, Swartz was served with a forfeiture warrant for property of JSTOR in his possession and refused to comply with the Court's warrant.<sup>10</sup> Swartz was indicted federally for wire fraud, computer fraud, and data theft, which was followed by the present Superseding Indictment on the same theories.

**III. MOTION TO SUPPRESS INTERCEPTIONS AND DISCLOSURES OF ELECTRONIC COMMUNICATIONS BY MIT PERSONNEL (No. 1)<sup>11</sup>**

Swartz first moves to suppress: (1) the historical guest registration, DHCP and IP address assignment and network routing records that MIT collected independently before January 4th as it sought to identify and locate the hacker; (2) the recording (or "packet capture") of the laptop's communications after it was found connected to MIT's network; and (3) the network's historical routing, addressing and switching records used to find the laptop after Swartz relocated it from Building 16 to the student center (Building W20) just before his arrest.

Apparently without a trace of irony, Swartz argues that MIT and law enforcement violated his rights to privacy as he hid his computers and hard drives in MIT's locked wiring closet, used pseudonyms to avoid identification, hard-wired his computers to MIT's network switch to avoid detection, siphoned off JSTOR's copyrighted documents, kept reconfiguring his computer to circumvent MIT's and JSTOR's efforts to keep him off their networks, and relocated the evidence to MIT's student center. In particular, Swartz asserts that the evidence listed above should be suppressed because the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, and the Fourth Amendment prevented MIT and

---

<sup>10</sup> Swartz later reached a civil agreement with JSTOR, pursuant to which he delivered to the Secret Service four hard drives containing millions of JSTOR's documents.

<sup>11</sup> Swartz's numbering convention is used here for ease of reference.

this expectation as (objectively) reasonable.

Swartz did not exhibit an actual, subjective expectation of privacy in MIT's network records. He has not submitted an affidavit declaring that he did. Nor could he credibly do so. Swartz is an experienced software engineer,<sup>12</sup> and thus understood that when he connected to MIT's and JSTOR's networks, his computer would send the networks his IP and MAC address information and that they would likely store that information as well.<sup>13</sup> In fact, Swartz demonstrated his subjective knowledge that MIT and JSTOR would record this information: when JSTOR blocked communications from Swartz's IP address, he changed his IP address by a single digit, and when MIT blocked his MAC address from obtaining a guest registration, he changed that by a single letter. And Swartz used a duplicitous name and email address when he sought a guest registration. He used and changed these identifiers precisely because he knew that his computer would disclose this type of information to MIT and JSTOR and that their networks would routinely log and record it.

Even if Swartz had truly believed that MIT would keep its computer records private, that expectation would not be "one that society is prepared to recognize as 'reasonable.'" *Smith v. Maryland*, 442 U.S. 735, 743 (1979) (quoting *Katz*, 389 U.S. at 361). In *Smith*, the Supreme Court concluded that neither installing nor using a pen register to collect information about the numbers dialed from the petitioner's home telephone constituted a search under the Fourth Amendment. In concluding that it did not constitute a search, the Supreme Court reasoned first

---

<sup>12</sup> See [http://en.wikipedia.org/wiki/Aaron\\_Swartz](http://en.wikipedia.org/wiki/Aaron_Swartz) (last visited Oct. 23, 2012) for his background.

<sup>13</sup> Indeed, MIT's IS&T (Information Services and Technology) DHCP Usage Logs Policy, quoted by Swartz at p. 7 of his motion, provided further notice that IP address, MAC address, and other information would be collected by the network. (Ex. 18).

that the petitioner could not have held any subjective expectation of privacy in the numbers that he had dialed because he knew that these numbers would be disclosed to a third party, the telephone company. *Id.* at 742. Even were this not the case, as the Supreme Court explained,

This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. In [*U.S. v. Miller*, 425 U.S. 435 (1976)], for example, the Court held that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business."

This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber.

*Id.* at 743-44 (citations omitted).

Just as in *Smith*, when Swartz used his computer, he knowingly and voluntarily gave information to a third party, MIT, so that electronic communications could be routed to and from his computer. This computer addressing, routing and switching information is merely the Internet equivalent of telephone numbering, cabling and subscriber information. When using MIT's network, Swartz assumed the risk that MIT would reveal this network connectivity information -- which contained no substantive content<sup>14</sup> -- to the police.

This was the conclusion in *United States v. Forrester*, 495 F.3d 1041 (9th Cir. 2007),

---

<sup>14</sup> Swartz claims that these records included the content of his communications, but that is easily disproved by reviewing the records, excerpted in Exs. 6-7. If you liken computer communications to documents sent via FedEx, these records disclose information about the envelope and the delivery tracking information you can see online, not the contents of the documents inside.

which ruled that law enforcement's discovery of Internet e-mail and IP addressing information is outside the scope of the Fourth Amendment. The court reasoned:

[E]mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communications. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on [sic] the users' imputed knowledge that their calls are completed through telephone switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of their websites they visited because they should know that these IP addresses are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties. Communication by both Internet and telephone requires people to "voluntarily turn[ ] over [information] to third parties."

495 F.3d at 1048-49 (citations omitted). Other appellate courts have reached the same conclusion. See *U.S. v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (holding defendant lacked reasonable expectation of privacy in his IP address because it is conveyed to and from third parties); *United State v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (holding that "subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation" because it is voluntarily conveyed to third parties); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (holding defendant identified no "evidence that he had a subjective expectation of privacy in his internet . . . 'subscriber information'" because he "voluntarily conveyed" that information to the company, and "assumed the risk" that the company would provide that information to the police (internal citations omitted)); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) ("We conclude that plaintiffs . . . lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the system's operators.").

Despite all these cases, Swartz urges that even if he lacked a reasonable expectation of privacy in other network addressing, routing and switching records, he had a reasonable expectation of privacy in the IP address that MIT gave him. In this regard, he invites the Court

to stretch the law of cell phone tracking to IP addresses, on the ground that MIT had configured its network so that knowing a computer's IP address would identify which campus building housed the computer. There is, however, no reasonable expectation of privacy in an IP address. See *Forrester*, 495 F.3d at 1048-49; *Christie*, 624 F.3d at 573-74. Further, even were the analogy apt, courts, including Judge Stearns in this District, have held that the Fourth Amendment does not protect *historical* cell tower location records. *In re Applications*, 509 F. Supp. 2d 76 (D. Mass. 2007) (Stearns, D.J.).<sup>15</sup> Here, MIT examined only historical IP records. So even were the cell phone analogy apt, it would not bolster Swartz's constitutional claim.

Swartz argues that MIT's policies created a reasonable expectation of privacy in MIT's DHCP logs. He has not averred, nor could he credibly aver, that he looked up and read MIT's written policy on DHCP log disclosure before he pseudonymously obtained a guest registration on their network. Without reading them, they could not create an expectation of any form on his part. Further, even if Swartz had read the policy, he would have read its warning that MIT might *disclose* the logs in compliance with a court order or a valid subpoena. The policy does not promise to disclose records *only* under those circumstances. Swartz cannot turn a warning that records might be disclosed to law enforcement into a guarantee of privacy.

---

<sup>15</sup> See also, e.g., *United States v. Dye*, 2011 WL 1595255, at \*9 (N.D. Ohio Apr. 27, 2011) (denying motion to suppress historical cell data); *United States v. Velasquez*, 2010 WL 4286276, at \*5 (N.D. Cal. Oct. 22, 2010) (same); *United States v. Benford*, 2010 WL 1266507, at \*3 (N.D. Ind. Mar. 26, 2010); *United States v. Suarez-Blanca*, 2008 WL 4200156, at \*8-\*11 (N.D. Ga. Mar. 26, 2008) (same); *Mitchell v. States*, 25 So. 3d 632, 635 (Fla. Dist. Ct. App. 2009) (same). But see *In re Application of the United States*, 620 F.3d 313, 317 (3d Cir. 2010) (asserting location information is not voluntarily conveyed to a cell phone provider but historical cell site records are "obtainable under a § 2703(d) order and that such an order does not require a traditional probable cause determination"); *In Re Application of the United States*, 809 F. Supp. 2d 113, 122-25 (E.D.N.Y. 2011); *In re Application of the United States*, 747 F. Supp. 2d 827 (S.D. Tex. 2010), appeal docketed, No. 11-20884 (5th Cir. Dec. 12, 2011).

2. ***Neither MIT Nor the Government Violated the Wiretap or Stored Communication Act By Collecting Non-Content Network Addressing, Routing and Switching Records***

As alternative bases for suppression, Swartz argues that MIT violated the Wiretap Act and that the Government and MIT both violated the Stored Communications Act.

a. ***No Statutory Suppression Remedies***

These statutory arguments fail from the outset because even had MIT or the Government violated these acts, neither act contains a suppression remedy for this type of case. Under the Wiretap Act, Congress provided a suppression remedy for violations involving wire and oral communications, but not those involving electronic communications, which are at issue here.<sup>16</sup> See *United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990); *United States v. Reed*, 575 F.3d 900, 915 (9th Cir. 2009); *United States v. Amanuel*, 615 F.3d 117, 125 (2d Cir. 2010). Meanwhile, Congress determined that suppression was inappropriate for violations of the Stored Communications Act under *all* circumstances. 18 U.S.C. § 2708; Wayne R. LaFare, Jerold H. Israel, Nancy J. King, and Orin S. Kerr, *Criminal Procedure* § 4.8(F) (3d ed. 2011) ("Importantly, the Stored Communications Act does not include a statutory suppression remedy for the unlawful acquisition or disclosure of records of the contents of communications, whether they are wire or electronic communications."). See also, e.g., *U.S. v. Perrine*, 518 F.3d at 1202; *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998).

With no suppression remedies, the motion to suppress must be denied.

---

<sup>16</sup> While wire and electronic communications may both be transmitted by wire, "wire communications" by definition convey a human voice, while "electronic communications" do not. See 18 U.S.C. § 2510 (1), (12), (18). None of the communications that Swartz seeks to suppress were spoken; all, accordingly, were electronic communications.

*b. No Violation of the Wiretap Act*

Even if the Acts theoretically allowed suppression, suppression would still be inappropriate because neither MIT nor the Government violated the Acts. MIT did not violate Title III by collecting routing and switching information in its network or by giving the Government historical network records that contained no "content." Title III prohibits the "interception" of oral, wire, and electronic communications. *See* 18 U.S.C. § 2510(1), (2), (4), (12). "Intercept" is defined as the "acquisition of the *contents* of any wire, electronic, or oral communication." § 2510(4) (emphasis added). "Contents" include only "information concerning the substance, purport, or meaning of that communication." § 2510(8). MIT did not violate the Wiretap Act in collecting logging records quite simply because the logs contain no "substance, purport or meaning" of Swartz's communications. Consider again excerpts from the guest registration, DHCP, and radius logs attached at Exs. 6-7. As is evident from the face of these mindless and frequently repetitive records, they do not contain any communications' contents. Rather, returning to the FedEx metaphor, these records contain information about the envelope, not the documents inside.

Swartz misreads *In re Application for an Order Authorizing use of a Pen Register and Trap*, 396 F. Supp. 2d 45 (D. Mass. 2005) (Collings, M.J.), to claim that "dialing, routing, addressing, and signaling information" regarding communications must also include the communications' contents. What Magistrate Judge Collings said is that "dialing, routing, addressing, and signaling information" concerning an Internet communication *might* contain the communication's contents if the information included an e-mail's subject line, a Google search's query terms, requested file names, or file paths. *See id.* at 48-49. What Magistrate Judge Collings also said is that if none of that information is included within the "dialing, routing,



addressing, and signaling information," then that information does not constitute contents. *Id.* Because the records included in Exs. 6-7 do not contain requests to JSTOR for its files, responses from JSTOR, or requests to websites such as Google for information, those records do not include contents and thus their disclosure could not violate the Wiretap Act.

*c. No Violation of the Stored Communications Act*

Nor did the Government violate the Stored Communications Act by obtaining MIT's historical network records without a warrant. The Stored Communications Act prohibits a provider of "electronic communication service to the public" from "divulg[ing] a record or other information pertaining to a subscriber to or customer of such service" to the government except "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2702(a)(3), (c)(3). Because of these qualifications, the Stored Communications Act simply did not apply.

*i. No service to "the public"*

To begin with, the Stored Communications Act does not apply to MIT because MIT does not provide an "electronic communication service to the public." *See generally* 18 U.S.C. § 2702 (emphasis added) (limiting voluntary disclosure of information by a provider of "electronic communication service to the public"). "The word 'public' . . . is unambiguous. Public means the 'aggregate of the citizens' or 'everybody' or 'the people at large' or 'the community at large. *Black's Law Dictionary* 1227 (6th ed. 1990)." *Anderson Consulting LLP v. UOP*, 991 F. Supp. 1041-42 (N.D. Ill. 1998) (interpreting Stored Communications Act, sometimes referred to as the Electronic Communications Privacy Act). "Thus the statute covers in it any entity that provides electronic communications (e.g., e-mail) service to the community at large." *Id.*

But MIT does not provide its computer services to the "aggregate of the citizens,"

"everybody," "the people at large," or "the community at large." Rather, MIT restricts use of its computer network to people who support MIT-sanctioned research and educational activities:

MIT's computing and network facilities and services are to be used for Institute purposes only and not for the benefit of private individuals or other organizations without authorization. Unauthorized access to the use of MIT computer and network services violates this policy.

See MIT's Policy on the Use of Information Technology ¶ 13.2.3 (Ex. 22). This policy is reiterated in MIT's Rules of Use of the network, which states that:

The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose.

(Ex. 4, § 1). These restrictions — which Swartz ignored during his crime and again in his brief — matter a great deal. "Providers do not provide services to the public if a person needs a special relationship with the provider to obtain an account." Wayne LaFare, Jerold Israel, Nancy King and Orin Kerr, *Principles of Criminal Procedure: Investigation*, § 3.11(e) (2d ed. 2009) (interpreting Stored Communications Act). Because MIT provided its network for the use of MIT's students, faculty and employees and their on-campus guests working with them on MIT-related pursuits, and MIT did not provide its network to everybody in Cambridge, MIT did not provide an "electronic communication service to the public." Consequently, MIT's disposition of its records does not fall under the Stored Communications Act.

ii. Swartz was not MIT's "customer" or "subscriber"

The Stored Communications Act is also inapplicable because Swartz was not MIT's customer or subscriber. The Act's restrictions on a provider of electronic communications services to the public from disclosing its communication records to law enforcement protect only the provider's "subscriber[s] or customer[s]." See 18 U.S.C. § 2702(a)(3). But Swartz was not

MIT's subscriber or customer. Swartz was not working on an MIT-related endeavor and instead gave MIT multiple false identities and identifiers. To call him MIT's subscriber or customer would be to call a shoplifter a "customer" or an airplane stowaway a "passenger."

Swartz says that he was MIT's subscriber or customer because MIT personnel repeatedly referred in internal and external communications to the hacker who was exfiltrating JSTOR's archive as a "guest." While MIT did refer to the hacker as a "guest," Swartz attributes too much to this usage. MIT referred to the hacker as a guest in order to identify the *type of account* that Swartz was using, not to verify that they had extended him an invitation.<sup>17</sup> Indeed, throughout this period no one even knew who "Gary Host" or "Grace Host" were, and no MIT personnel had "invited" Swartz to meet in MIT's restricted wiring closet or invited him to connect directly to MIT's network switch. The term "guest" was being used simply in contradistinction to an identifiable faculty member, student or employee. Consequently, Swartz was not a protected "subscriber" or "customer" under the statute and he cannot claim the statute's protections.

Even if Swartz could somehow claim to have been MIT's subscriber or customer when he first registered his computer on September 24, 2010, he lost that status on September 27, 2010, after the first two large download incidents, when MIT banned his network access through the MAC address block. And Swartz lost it again when MIT banned him again on October 13, 2010.

### *III. Proper disclosures to protect MIT's rights and property*

Finally, even if MIT had been a provider "to the public" and even if Swartz had been MIT's subscriber or customer, MIT properly complied with the Stored Communications Act by

---

<sup>17</sup> Nor could Swartz claim that MIT's e-mails to JSTOR misled him into thinking that he was a guest, since he was not a party to those e-mails.

providing the Government records in order to protect its rights by locating and identifying the hacker. Under the Stored Communications Act, MIT could lawfully disclose the necessary records as "necessarily incident to the rendition of the [electronic communications] service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2702(c)(3). Disclosures by service providers such as MIT are held to the standard of reasonableness. See *United States v. Harvey*, 540 F. 2d 1345, 1350 (8th Cir. 1976) (interpreting similar language in the wiretap statute found at 18 U.S.C. § 2511 (2)(a)(i)).

MIT wanted to rid its network of Swartz, or else MIT would not have banned his MAC addresses and installed a videocamera in his hiding place. And MIT had good reasons to rid itself of Swartz: his actions had resulted in MIT's JSTOR service being shut off and MIT researchers' being denied access to research materials. Thus, MIT was protecting not just JSTOR's rights, as Swartz claims, but also MIT's own rights in its network, its interest in using that network to provide its researchers JSTOR articles, and its contract with JSTOR to provide JSTOR's articles over its network. Under § 2702(a)(3), MIT's disclosures were proper.

Swartz argues that MIT's disclosure of network records to law enforcement under § 2703(c)(3) was not "necessarily incident" to protecting MIT's network because MIT could have protected itself simply by removing his computer from the wiring closet. But MIT had no such assurance. The hacker had repeatedly re-accessed the network after direct efforts to stop him. As far as MIT knew, taking away his computer would merely spur him to return with more equipment yet again. Instead, MIT had to identify the hacker and assist with his apprehension in order to prevent further abuse. Providing the Government these records was necessarily incident

to identifying the hacker and thus protecting MIT's rights and property under § 2703(c)(3).<sup>16</sup> Consequently, MIT acted properly when it disclosed these records to law enforcement both consensually at the outset and later pursuant to a subpoena.

**B. The Packet Capture of the Laptop's Communications<sup>19</sup>**

Unlike the other records that Swartz's first motion attempts to suppress, the packet capture of the laptop's communications did involve intercepting the communications' contents. Unlike the system logs discussed above, intercepting the contents of electronic communications usually requires a Title III order, absent an exception.

There is an applicable exception here, however, because Swartz was a trespasser on MIT's system during the packet capture on January 4th. As a matter of constitutional law, a trespasser lacks a reasonable expectation of privacy in a place he has no legitimate right to be. *Rakas v. Illinois*, 439 U.S. 128, 143-44, n.12 (1978) (no legitimate expectation of privacy where a person's presence is wrongful); *United States v. Curlin*, 638 F.3d 562, 565 (7th Cir. 2011) (defendant had no reasonable expectation of privacy in house from which he had been

---

<sup>16</sup> Swartz also contends that MIT's disclosure of its routing and trafficking records violated his Fourth Amendment rights, citing *Crispin v. Christian Audigier, Inc.* 717 F. Supp. 2d 965 (C.D. Cal. 2010); and *In re United States*, 665 F. Supp. 2d 1210 (D. Or. 2009). These cases are inapposite because they did not consider the application of § 2702(c)(3). However, even if MIT had violated the Stored Communications Act by providing the Government its historical routing and registration records without a warrant, doing so would not have rendered the Government's acquisition of those records a *per se* unreasonable search under the Fourth Amendment. See *City of Ontario California v. Quon*, 130 S. Ct. 2619, 2632 (2010) ("Respondents point to no authority for the proposition that the existence of statutory protection [under the Stored Communications Act] renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise.").

<sup>19</sup> No derivative use has been made of this packet capture, and at the present time, the Government does not intend to introduce it in its case-in-chief. The Government responds, however, to preserve its right to use this evidence should it become material.

evicted); *United States v. Sanchez*, 635 F.2d 47, 64 (2d Cir. 1980) (“[A] mere trespasser has no Fourth Amendment protection in a premises he occupies wrongfully.”); *Amezquita v. Hernandez-Colon*, 518 F.2d 8, 11 (1st Cir. 1975) (squatters formerly evicted from public land had no expectation of privacy in homes they unlawfully constructed there); *United States v. Gale*, 136 F.3d 192, 195 (D.C. Cir. 1998) (individual lacked legitimate expectation of privacy in apartment he occupied without permission of its tenant or other legal authority); *United States v. Rambo*, 789 F.2d 1289, 1295-95 (8th Cir. 1986) (hotel occupant asked to leave by police officers acting for hotel management no longer had a reasonable expectation of privacy in hotel room).

Swartz was a trespasser in every sense of the word. To physically get to the network he passed doors with “no trespassing” signs, went into a basement corridor and opened locked steel doors to hide in a restricted wiring closet. Then, having accessed the network using pseudonyms, Swartz repeatedly manipulated his computer’s MAC address as MIT repeatedly barred its use on their network. As a trespasser, then, Swartz had no constitutional expectation of privacy in the electronic communications being sent to and from his computer in the wiring closet.

Title III integrates the constitutional trespasser exception in a statutory exception to its order requirement:

- (i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer if--
  - (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser’s communications on the protected computer;
  - (II) the person acting under color of law is lawfully engaged in

an investigation;

- (III) the person acting under the color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
- (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

18 U.S.C. § 2511(2)(i).<sup>20</sup>

The packet capture here fits the statutory exception. First, MIT authorized it. § 2511(2)(i)(I). Second, the packet capture was performed by "a person acting under color of law engaged in an investigation," § 2511(2)(i)(II); although MIT personnel initiated the packet capture, law enforcement investigators called to the scene concurred that it should continue. Third, MIT and law enforcement investigators "had reasonable grounds to believe that the contents of the computer trespasser's communications w[ould] be relevant to the investigation," § 2511(2)(i)(III), by helping to identify who owned the ghost laptop and what unlawful activities the computer was conducting on the network. Finally, the packet capture was set up so that it

---

<sup>20</sup> Swartz's Wiretap Act argument in Motion to Suppress No. 1 analyzes a different exception, the provider exception set forth in 18 U.S.C. § 2511(2)(a)(i). See Def.'s Motion to Suppress No. 1 at 8-14. That analysis centers on Swartz's misguided notion that MIT acted only to protect JSTOR, and not itself, as well. As discussed above in the context of the Stored Communications Act, *supra* at 22-23, this is incorrect: MIT was not just protecting JSTOR's rights, but also MIT's own rights in its network and in its contract with JSTOR to provide JSTOR's articles over MIT's network. Accordingly, for the same reasons articulated *supra* at 22-23, MIT had the right to intercept and disclose to law enforcement the communications over its network to and from the ghost laptop to protect MIT's rights and property. 18 U.S.C. § 2511(2)(a)(i). Swartz's objection to using the provider exception should be overruled.

Swartz analyzes the Wiretap Act's trespasser exception, 18 U.S.C. § 2511(2)(i), in his Motion to Suppress No. 2 at 17-18.

"d[id] not acquire communications other than those transmitted to or from the computer trespasser." § 2511(2)(i)(IV).

Here, too, Swartz unsuccessfully seeks to paint himself as MIT's guest rather than as its computer trespasser. See Def.'s Motion to Suppress No. 2 at 17-18. A "computer trespasser" is "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer," 18 U.S.C. § 2510(21)(A), and "does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer," § 2510(21)(B). Again, it is disingenuous for Swartz to claim that he was MIT's invitee after MIT had repeatedly cut off his computer's connection. Neither Swartz's ability to fake his way onto the system nor MIT's referring to his logon account as a guest turned him into an invitee. *See supra* at 21-22 (discussing MIT's and JSTOR's efforts to ban Swartz). Certainly he was not "a person known by the owner or operator of [MIT's network] to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer." § 2510(21)(B).

Accordingly, MIT and the Government met each of the elements of § 2511(i)'s trespasser exception to the wiretap order and a Title III order was not necessary to monitor the ghost laptop's communications.

#### **IV. MOTION TO SUPPRESS FRUITS OF WARRANTLESS SEARCHES (No. 2)**

After MIT tracked the JSTOR downloads to the laptop in the closet, MIT called the police. When the Cambridge Police and Secret Service arrived, they processed the scene for



fingerprints and unsuccessfully attempted to copy volatile evidence in the computer's random access memory ("RAM") which would be destroyed if the computer were turned off.

Swartz's Motion to Suppress No. 2 moves to suppress the fruits of each of these investigative steps.<sup>21</sup> This motion is meritless and should be denied. Swartz lacked a reasonable expectation of privacy in equipment hidden on somebody else's property. The officers were lawfully in MIT's wiring closet, where the laptop and hard drive were in plain view. Exigent circumstances justified the attempt to capture the contents of the laptop's RAM before it was powered down. In any event, this aspect of Swartz's motion is moot because law enforcement officers were unable to copy the RAM.

**A. Swartz Lacked a Reasonable Expectation of Privacy in MIT's Wiring Closet and Student Center Office and the Things He Hid There**

Swartz lacked a reasonable expectation of privacy in the laptop and hard drives that he hid in MIT's wiring closet and student center office. He placed the computer where he and it had no right to be, and left the equipment unattended for extended periods while it robotically stole massive portions of JSTOR's database. The equipment was an instrumentality of a crime, being used in an ongoing crime, when crime scene investigators opened the laptop and hard drive cases on January 4, 2011 and seized them on January 6, 2011.

**1. *Whatever Swartz's Claimed Subjective Expectation of Privacy in Instrumentalities of Ongoing Crime Hidden in a Victim's Locked Utility Closet and Office, It Is Not One That Society Is Objectively Prepared to Recognize***

Whatever subjective expectation of privacy Swartz may have had by using bogus

---

<sup>21</sup> Motion to Suppress No. 2 also seeks again to suppress the results of the packet capture. Those arguments are dealt with in the Government's response to Motion to Suppress No. 1.

Indeed, the Government sought and obtained a warrant for this purpose.

It was also proper under the exigent circumstances described below.

**B. Exigent Circumstances Justified an Attempt to Copy the Laptop's RAM**

When MIT and the officers arrived at the wiring closet on January 4, 2011, they did not know who had connected the laptop to MIT's network, whether it was being used for any other illegal purposes in addition to the downloads, or how soon the hacker might return and take the laptop. After crime scene specialists had fumed the laptop for fingerprints, Special Agent Pickett sought, unsuccessfully, to copy the laptop's Random Access Memory ("RAM").<sup>24</sup> This was lawful. "Government agents may conduct a warrantless search or seizure if (1) probable cause supports the search or seizure and (2) 'exigent circumstance' exist. Exigent circumstances include imminent destruction of evidence, a threat to the safety of law enforcement officers or the general public, 'hot pursuit' of a suspect by police, or likelihood that suspect will flee before the officer can obtain a warrant." 41 Geo. L.J. Ann. Rev. Crim. Proc. 83 (footnote omitted, collecting cases). *See also Schmerber v. California*, 384 U.S. 757, 766-72 (1966) (exigent circumstances justified warrantless search of blood sample to test alcohol level because police had probable cause to arrest and feared destruction of the evidence by dissipation of alcohol in

---

communicate. *See supra* at 15-17. Nevertheless, the Government does not intend to offer this information in evidence in its case-in-chief and therefore this aspect of his motion is moot.

<sup>24</sup> Law enforcement officers are not uniformly clear as to whether the laptop's screen was showing a logon screen when they opened the laptop to fingerprint it or whether the logon screen appeared only when they attempted to copy the laptop's RAM. Regardless, officers legitimately opened the laptop's cover for the multiple reasons described above, putting the logon screen in plain view. If the logon screen did not appear until officers touched the laptop's keyboard, touching the keyboard was lawful under *Hicks* – there was probable cause to believe that the logon screen would show evidence of who owned the laptop.

the blood). "Exigent circumstances occur when a reasonable officer could believe that to delay acting to obtain a warrant would, in all likelihood, permanently frustrate an important police objective, such as to prevent the destruction of evidence relating to criminal activity . . . ."

*United States v. Rengifo*, 858 F.2d 800, 805 (1st Cir. 1988).<sup>25</sup>

Agent Pickett was reasonable in his belief that if officers delayed copying the RAM while they obtained a warrant, they might permanently lose access to significant evidence. A computer contains two types of information: information stored on the hard disk remains after the computer is turned off, whereas information stored in RAM is completely lost when the computer is turned off. Despite its volatility, RAM information can assist an investigation in several ways, including providing the computer's decryption passwords. Without these passwords, the computer can for all intents and purposes be impossible to search later, despite having a valid search warrant. Accordingly, exigent circumstances justified Special Agent Pickett's efforts to copy the laptop's RAM without a warrant before the perpetrator could access his computer again and power it down.

To copy the RAM, officers needed to access the computer's screen and keyboard. Viewing the laptop's screen was merely incidental to the lawful exigent effort to copy the laptop's RAM.

---

<sup>25</sup> In an analogous situation, courts have repeatedly upheld searching a cell phone's call log incident to arrest on the grounds that incoming calls can cause the least recent calls to be erased. See e.g., *United States v. Valdez*, 2008 WL 360548 (E.D. Wis. 2008); *United States v. Mercado-Nava*, 486 F.Supp. 2d 1271, 1278 (D. Kan. 2007); *United States v. Parada*, 289 F. Supp. 2d 1291, 1303-04 (D. Kan. 2003).

**C. Discovery Was Inevitable After Officers Obtained Warrants to Search Seized Equipment**

Even had a warrant been necessary to search the laptop and hard drive on January 4th, the results of these searches would have been discovered inevitably after the officers obtained warrants to search them later on. "Although evidence derived from unlawful searches is generally subject to suppression, there are numerous exceptions to this rule. One such, the inevitable discovery exception, applies to any case in which the prosecution can show by a preponderance of the evidence that the government would have discovered the challenged evidence had the constitutional violation to which the defendant objects never occurred." *United States v. Scott*, 270 F.3d 30, 42 (1st Cir. 2001) (citing *Wong Sun v. United States*, 371 U.S. 471, 484-87 (1963) and *Nix v. Williams*, 467 U.S. 431, 440-48 (1984)). The inevitable discovery rule has three factors:

[A]re the legal means truly independent; are both the use of the legal means and the discovery by the means truly inevitable; and does the application of the inevitable discovery exception either provide incentive for police misconduct or significantly weaken Fourth Amendment protection?

*United States v. D'Andrea*, 648 F.3d 1, 12 (1st Cir. 2011) (quoting *United States v. Silvestri*, 787 F.2d 736, 744 (1st Cir. 1986)).

The Government obtained warrants to search the laptop and hard drive on February 24<sup>th</sup>, evincing its intention that the two would inevitably be searched. The warrants were independent of the January 4th searches: their affidavits did not rely upon or even refer to the fingerprints, what was seen on the laptop screen, or the contents of the packet capture. Finally, there was no police misconduct (intentional or unintentional) that would be encouraged by applying the inevitable discovery doctrine.

Accordingly, if the Court determines that any evidence recovered on January 4th was recovered unlawfully, the Court should nonetheless find it admissible because it would inevitably have been discovered when the independently obtained lawful warrants were subsequently executed.

**V. MOTION TO SUPPRESS FRUITS OF UNLAWFUL ARREST AND SEARCH OF HP USB DRIVE (No. 3)**

Swartz next moves to suppress the USB drive recovered incident to his arrest and subsequently searched pursuant to a warrant. His USB drive contains a version of the software that Swartz used to download JSTOR's articles. This motion must be denied because there was probable cause both to arrest Swartz on January 6, 2011, and to search the USB drive recovered from his backpack incident to his arrest.

**A. Probable Cause to Arrest Aaron Swartz on January 6, 2011**

***1. Facts Known at the Time of Arrest***

When MIT Police Captain Albert Pierce and others arrested Swartz on January 6, 2011, there were facts sufficient to establish probable cause that Swartz had committed several crimes. At a minimum, arresting officers knew, as reflected in the report attached to the initial charging complaint (Ex. 19):

- (1) A person had entered a restricted telephone and networking closet whose access was controlled by MIT;
- (2) That person had connected a laptop and external hard drive directly to a networking switch without authorization;
- (3) That person had hidden the equipment under a cardboard box;
- (4) The laptop had illegally downloaded scientific periodicals from JSTOR;
- (5) The person had downloaded gigabytes of data from JSTOR, valued in the

tens of thousands of dollars at the time;

- (6) The suspect he was about to interview looked just like the person who had just been seen on a video removing the equipment from the closet;
- (7) The suspect was near MIT, the scene of the crime; and
- (8) The suspect he was about to interview fled when approached by police.

**2. *Probable Cause to Arrest for Federal and State Computer Crime Violations, Among Others***

On these facts, officers had objective probable cause to believe that Swartz had accessed MIT's computer system without authorization and thereby taken substantial amounts of data from JSTOR. Thus, at the time of arrest, they had objective probable cause to believe that Swartz had violated at least two computer crime statutes: Massachusetts General Laws ch. 266, § 120F and 18 U.S.C. § 1030(a)(2)(C). There was probable cause to believe that Swartz had violated the state computer crime statute, because it punishes "[w]hoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access," Mass. Gen. Laws ch. 266, § 120F. There was probable cause to believe that Swartz had violated the federal computer crime statute, because it similarly punishes whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains — (C) information from any protected computer," 18 U.S.C. § 1030(a)(2)(C). Swartz has not challenged, nor can he, the existence of probable cause to believe at the time of his arrest that he had committed state and federal computer crimes. Since officers had objective probable cause to arrest Swartz, the search instant to his arrest that recovered the USB drive from his backpack was also lawful.

Moreover, in addition to the computer crime statutes, the facts listed above also gave objective probable cause to believe that Swartz had violated all the other statutes on which he was later indicted: breaking and entering in the daytime with intent to commit a felony in violation of Massachusetts General Law ch. 266, § 18; larceny over \$250 in violation of Massachusetts General Laws ch. 266, § 30; wire fraud in violation of 18 U.S.C. § 1343; computer fraud in violation of 18 U.S.C. § 1030(a)(4); and reckless damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5).

**3. *The Officers' Subjective Assessment of Probable Cause is Irrelevant***

Swartz says that the officers lacked probable cause to arrest him for the state breaking and entering statute because the statute did not cover his conduct and they did not identify any other applicable criminal statutes at the time.

But the officers' *subjective* intent at the time of an arrest is irrelevant. An arrest and a search incident thereto are valid if the arresting officer had objective grounds for probable cause to arrest the defendant, even if the officer subjectively mistook which statute applied. *E.g.*, *Devenpeck v Alford*, 543 U.S. 146, 153-54 (2004) (holding that the "[s]ubjective intent of the arresting officer . . . is simply no basis for invalidating an arrest. Those are lawfully arrested whom the facts known to the arresting officers give probable cause to arrest."); *United States v. Bookhardt*, 277 F.3d 558, 565 n.10 (D.C. Cir. 2010) (holding that existence of probable cause to arrest must be determined objectively from facts and circumstances known to officers at time of arrest without regard to subjective intentions of officers involved).<sup>26</sup> The officers' subjective

---

<sup>26</sup> See, similarly, *Barna v. City of Perth Amboy*, 42 F.3d 809, 819 (3d Cir. 1994) (holding that "[p]robable cause need only exist as to any offense that could be charged under the circumstances"); *United States v. Kalter*, 5 F.3d 1166, 1168 (8<sup>th</sup> Cir. 1993) (upholding arrest

intent is irrelevant even if they mistakenly charged a defendant with a state crime but had objective probable cause to believe that the defendant had committed a federal crime. *See United States v. Pollack*, 739 F.2d 187, 199 (5<sup>th</sup> Cir. 1984) ("If, as in the instant case, the arresting officer knows facts which constitute probable cause to believe that the suspect has committed a federal crime, it is not required that the officers subjectively believe that probable cause exists to arrest for that crime. Thus [the agent's] mistaken belief regarding a \$5,000 [federal] jurisdictional requirement is not fatal.").

Consequently, the Court should focus on the fact that the officers had objective probable cause to arrest Swartz on the various statutes listed above and should ignore the officers' identification of different statutes at the time of arrest.

**4. *Officers Nonetheless Had Probable Cause to Arrest Swartz for Breaking and Entering with Intent to Commit a Larceny***

Even were the arresting officers' subjective intent relevant, the officers had probable cause to arrest Swartz for breaking and entering in the daytime with intent to commit larceny.

Swartz claims that he could not have committed this offense because he believed he had permission to be in the wiring closet. Whether Swartz believed that he had MIT's permission to be in the closet is beside the point, because the *officers* had probable cause to believe that Swartz

---

because, although the police lacked probable cause to arrest defendant for concealed-weapon violation that was actual reason for the arrest, police nevertheless had probable cause to arrest him for violating a separate ordinance requiring that a gun be carried in a locked container); *United States v. Atkinson*, 450 F.2d 835, 838 (5<sup>th</sup> Cir. 1971) (declining to decide whether an arrest for false pretenses was legal because the officer had probable cause to arrest the defendant for operating a vehicle with an invalid license tag); *Kingler v. United States*, 409 F.2d 299, 303-06 (8<sup>th</sup> Cir. 1969) (upholding arrest because, although the police lacked probable cause to arrest the defendant for vagrancy, the charged offense, they had probable cause to believe that he had committed robbery); *see also* Wayne R. LaFare, *Search and Seizure* § 1.4(d) (3d ed. 1996) (collecting cases).



lacked permission and knew that he lacked permission.

Swartz also argues that he could not have committed a larceny because he did not "intend to deprive JSTOR of its property permanently, nor did the downloading have that effect."

Swartz misinterprets the larceny statute. Massachusetts General Law chapter 266, § 30 was specifically amended in 1983 to include electronically processed or stored data to ensure that prosecutors could use it to prosecute the then-nascent problem of computer crime. Subsection 2 of the law now states, in pertinent part, that "'Property', as used in [section 30], shall include . . . electronically processed or stored data, either tangible or intangible, data in transit [and] telecommunications services." Mass. Gen. Laws ch. 226, §30 (2). As stated by Representative Kenneth Lemanski in a letter to the governor's legislative office (Ex. 20):

The most important aspect of this bill, in my opinion, is the fact that it now allows electronic impulses to be defined as property. This is essential to combating computer crime. . . [Prosecutors] will now be able to refer to a specific statute in the prosecution of what was formerly one of the most difficult types of crime. H.6227 directly attacks what, up until now, had been the judicial sticking point: are electronic data "property"? Our own Supreme Judicial Court agreed with earlier Federal Opinions that the answer was no, under the existing statutes. H.6227 remedies this by explicitly including computer data in the definition of property.

Thus understood, the statute does not exclude from coverage a hacker who copies his victim's data. Nor should this Court make such a novel interpretation of Massachusetts law. "A statute should be constructed [to give effect] to all of its provisions, so that no part will be inoperative or superfluous, void or insignificant." *Corley v. U.S.*, 556 US 303, 304 (2009). "It is an elementary rule of construction that effect must given, if possible, to every word, cause and sentence of a statute." 2A *Sutherland Statutory Construction* § 46.06 (7<sup>th</sup> ed. 2007). All computer data theft involves copying. If the statute were interpreted to punish the data thief only if he erased the

victim's data, that would render the computer crime amendment largely inoperative.

In sum, at the time of arrest, there was objective probable cause to believe that Swartz had violated the state and federal computer crime statutes, plus several other state and federal statutes, including breaking and entering to commit larceny. The arrest and the seizure of the USB drive incident to arrest were therefore lawful.

**B. Probable Cause to Search the USB Drive**

After the USB storage drive was seized incident to Swartz's arrest, the Government obtained a warrant to search the drive for violations of 18 U.S.C. § 1030(2)(2) (data theft); 18 U.S.C. § 1030(a)(5)(A) (intentional damage to a computer system) and 18 U.S.C. § 1343 (wire fraud). The Government then searched the drive pursuant to that warrant.

Swartz incorrectly contends that officers lacked probable cause to believe that the USB drive contained evidence of Swartz's crimes. A magistrate's decision to issue a warrant must be reviewed with great deference. A reviewing court should give significant deference to the magistrate judge's initial evaluation of an affidavit for a search warrant, reversing the magistrate judge only when there is no "substantial basis" for concluding that probable cause existed. *United States v. Ribetiro*, 397 F.3d 43, 48 (1st Cir. 2005) (citing *United States v. Felix*, 182 F.3d 82, 86 (1st Cir. 1999)).

Moreover, Magistrate Judge Dein's conclusion that officers had probable cause to believe that the USB drive contained evidence was amply supported by the affidavit. As set forth in the affidavit (Ex. 21), Swartz had been videotaped entering the wiring closet on January 4, 2011, and again on January 6, 2011, shortly before he was arrested. (Aff. ¶¶ 22, 24.) He was arrested near MIT, the scene of the crime, shortly after the "ghost laptop" had been relocated to MIT's

Building W20. (Aff. ¶ 25). The crime involved using a program to download a large amount of information. (Aff. ¶¶ 12-19.) USB drives are frequently used to store software, data and records, including the type of records that were illegally downloaded from JSTOR. (Aff. ¶ 26). USB drives are also frequently used to transfer records and data between computers and hard drives, and Swartz had used two laptops on October 9, 2010. (Aff. ¶¶ 17, 18, 26). Because Swartz was arrested on the afternoon of the day he was last seen in the wiring closet, there was reason to believe that he had the USB drive with him as he committed the crime.

Probable cause does not require a certainty of finding evidence. All that is needed is a "reasonable likelihood" that incriminating evidence will turn up during a proposed search. *United States v. Clark*, 685 F.3d 72, 76 (1st Cir. 2012). The facts set forth above established a more than reasonable likelihood that the USB drive would hold records relevant to the crime.

Even assuming that Agent Pickett's search warrant affidavit was lacking, the evidence seized pursuant to the warrant should nonetheless be admitted under the good-faith doctrine enunciated in *United States v. Leon*, 468 U.S. 897, 922 (1984). In *Leon*, the Supreme Court held that evidence seized in good-faith reliance on a warrant later found defective is admissible at trial. *Id.* There are four exceptions in which the good-faith exception may not be invoked: (1) when the magistrate was misled by false information that the affiant knew was false or should have known was false but for his reckless disregard for the truth; (2) when the magistrate wholly abandoned her neutral role; (3) when the affidavit is so lacking in indicia of probable cause that no reasonable officer could believe to the contrary; and (4) when a warrant is so facially invalid, as by failing to describe with particularity the premises to be searched, that no reasonable officer could believe it valid. *Id.* at 923; see also *United States v. Owens*, 167 F.3d 739, 745 (1st Cir.

1999). Here, none of those exceptions is present, and thus, even assuming *arguendo* that the search warrant affidavit was deficient, the Court should rule the evidence derived from the warrant is admissible.

**VI. MOTION TO SUPPRESS RESULTS OF SEARCHES OF SWARTZ'S APARTMENT AND OFFICE (No. 4)**

Swartz's fourth motion to seeks to suppress the results of the searches of his apartment and his office, even though those searches were performed subject to search warrants. Because the Government will not introduce any evidence from the searches during its case in chief, nor evidence derived from those searches, this motion is moot.

The Government reserves the right to cross-examine Swartz about his statements and actions during and after those searches if he testifies on his own behalf.<sup>27</sup>

**VII. MOTION TO SUPPRESS FRUITS OF SEARCHES OF SEIZED COMPUTER EQUIPMENT (No. 5)**

Swartz's final motion seeks to suppress the searches of the laptop and the hard drive that were seized on MIT's property and the USB drive that was seized from Swartz incident to his arrest, all of which were searched pursuant to federal search warrants. Swartz seeks suppression because, he contends, the Government should have obtained and executed the warrants sooner, and thereby the Government unlawfully interfered with his possession of his equipment.

The motion should be denied. Having left the equipment unattended for months at MIT, having had it properly seized as physical evidence by the police under exceptions to the Fourth

---

<sup>27</sup> Even were the defendant's statements derivative of a Fourth Amendment violation — which they were not — they would be admissible for impeachment purposes. See e.g., *U.S. v. Torres*, 926 F.2d 321, 323 (3rd Cir. 1991) (evidence obtained in violation of Fourth Amendment admissible to impeach defendant's testimony).

Amendment's warrant requirement, and having not sought the equipment's return before the warrants' issue, any rights that Swartz might theoretically have had to the equipment's return were not meaningfully infringed while the Cambridge Police Department held the evidence in their case and the Secret Service sought warrants to search them for their federal investigation.

**A. Swartz Claims that the Police Improperly Held the Equipment After He Was Arrested and Charged**

Swartz asserts an unusual basis for relief in his fifth motion to suppress. He does not argue here that the equipment was seized improperly or that the warrants failed to articulate probable cause to believe that the equipment contained evidence of a crime.<sup>28</sup> Rather, he argues solely that the officers' delay in obtaining the warrants unreasonably interfered with his possessory interests. See Def.'s Motion to Suppress (No. 5) at 3 ("[E]ven a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution infringes *possessory interests* protected by the Fourth amendment's prohibition on 'unreasonable searches.'" (quoting *United States v. Jacobson*, 466 U.S. 110, 124 (1984)) (emphasis added). See also *United States v. Burgard*, 675 F.3d 1029, 1033 (7<sup>th</sup> Cir. 2012) ("On the individual person's side of this balance [of reasonableness], the critical question relates to any possessory interest in the seized object, not to privacy or liberty interests. A seizure affects only the person's possessory interests; a search affects a person's privacy interests.") (internal quotation marks and citations omitted), *cert. denied*, 2012 WL 2002441 (Oct. 1, 2012).

In other words, this motion focuses not on what the officers found inside the equipment, or even how they found it, but rather on the Cambridge Police Department's retention of the

---

<sup>28</sup> To the extent that the motion does raise these arguments, the Government disposed of them when responding to Swartz's earlier motions to suppress.

equipment in a pending state criminal case before the Secret Service obtained and executed warrants in the federal investigation.

**B. *The Cambridge Police Properly Seized and Held the Laptop, Hard Drive and USB Drive as Physical Evidence***

The Cambridge Police Department properly seized and held the laptop, the hard drive, and the USB drive as *physical evidence* in their state case under exceptions to the Fourth Amendment's warrant requirement. The equipment constituted physical evidence of computer crimes, larceny, and breaking and entering, just as a bag of burglar tools or a bag of stolen goods would be physical evidence if recovered at the scene of a crime or if seized incident to a burglar's arrest. *See supra*. The police accordingly had an objective basis to deprive Swartz of possession of the equipment throughout the period they held it in their evidence locker, a basis that was wholly independent of the Secret Service's subsequent searches of the equipment's contents.

Swartz does not contend — nor could he credibly contend — that the Cambridge police had an insufficient basis for continuing to hold the laptop and hard drive as physical evidence pending trial, even if the Secret Service had never obtained warrants to examine their contents. The laptop and the hard drive were in the closet to which the unauthorized downloads had been traced. A physical wire extended from the laptop and hard drive to MIT's network, and a virtual wire connected MIT's network to JSTOR's database. The laptop could be used to conduct the unauthorized downloads — the burglar's tools — and both the laptop and the hard drive could be used to store the articles — the loot. In this sense, they were the last physical links in the theft of JSTOR's articles. And they were instrumentalities of a crime which need not have been returned to the suspected perpetrator.

While one step removed, the Cambridge police had a sufficient basis to continue to hold the USB drive seized from Swartz incident to his arrest as physical evidence, as well. Swartz was arrested near MIT, within hours of having last been seen in the wiring closet. His crime involved the use of a program to download a large amount of information. USB drives are frequently used to store software applications, data and records, including the type of records that were illegally downloaded from JSTOR. They are also frequently used to transfer records and data between computers and hard drives, and MIT's records indicated that the perpetrator had used two laptops when executing his crime on October 9, 2010. *See supra*.

When an officer lawfully seizes property without a warrant because of probable cause to believe that it constitutes evidence of a crime, the officer may hold on to that evidence without a warrant and therefore the defendant has no grounds to complain that the officers delayed in searching it. *See United States v. Carter*, 139 F.3d 424, 426 (4th Cir. 1998) (en banc) (denying motion to suppress because of excessive delay between seizure of suitcase incident to arrest and issuance of search warrant, because the suitcase itself was evidence of the crime apart from the suitcase's contents); *United States v. Wright*, 2010 WL 841307 at \*8-\*10 (E.D. Tenn. Mar. 3, 2010) (holding almost month-long delay between seizure of laptop computer and application for warrant not unreasonable, because the laptop had evidentiary value in and of itself, apart from its contents, since the suspect's pre-arrest communications made it probable that the suspect would arrive at a destination with a computer); *id.* at \*9 ("And as *Mitchell* itself indicates, the Government is under no obligation to return property if it has 'some other evidentiary value.'") (quoting *United States v. Mitchell*, 565 F.3d 1347, 1352 (11th Cir. 2009)). Cases that Swartz cites for the contrary position are typically factually inapposite in one of two critical respects:

either the court never considered whether the searched computer or cellphone was physical evidence of a crime independent of its contents, or the court rejected the argument that the equipment was physical evidence of the crime.<sup>29</sup> Others are even less germane narcotics cases.<sup>30</sup> In sum, there was no infringement of Swartz's possessory interests in the computer equipment before it was searched pursuant to federal warrants, because it was being lawfully held during this time as physical evidence and instrumentalities of criminal activity.

**C. *Swartz Never Asked for Any of the Equipment Back During the Period He Now Claims His Possessory Interests Were Wrongfully Infringed Upon***

At no time before the warrants were issued did Swartz or his counsel seek the return of

---

<sup>29</sup> See *United States v. Burgard*, 675 F.3d 1029 (7th Cir. 2012) (cellphone seized on probable cause to believe that the phone would contain evidence of a crime; no argument that the phone was evidence of a crime apart from its contents); *United States v. Mitchell*, 565 F.3d 1347, 1352 (11th Cir. 2009) (noting that the government would not have been obligated to return the computer if it had evidentiary value apart from its contents; no argument for that the computer was evidence apart from its contents); *United States v. Rubinstein*, 2010 WL 2723186 at \*12-14 (S.D. Fla. June 24, 2010) (no argument computer seized at the border was evidence independent from the files it contained); *United States v. Riccio*, 2011 WL 4434855 (S.D. Cal. Sept. 23, 2011) (no argument that phone was evidence apart from its contents); *United States v. Shaw*, 2012 WL 844075 at \*3 (N.D. Ga. May 25, 2012), (evidentiary value of cellphones seized incident to an arrest in a drug conspiracy was not readily apparent without regard to the information to be found in the telephones).

One case cited by Swartz, *United States v. Budd*, 549 F.3d 1140, 1147-48 (7th Cir. 2008), actually helps the Government because it holds that even if officers waited too long in obtaining a warrant to seize a computer, the search of the computer pursuant to the warrant would not be suppressed under the independent source doctrine if the affidavit was premised on information that had not been obtained from the computer during its illegal detention.

<sup>30</sup> See *United States v. Jacobson*, 466 U.S. 109, 122, 124-25 (1984) (affirming that officer may seize property without a warrant based on probable cause to believe that it contains contraband and that officers did not need a warrant to destroy a small amount of suspected cocaine to perform a field test); *Segura v. United States*, 468 U.S. 796 (1984) (holding that officers who had probable cause to believe an apartment contained a criminal drug operation but entered illegally, nevertheless did not violate the Fourth Amendment by securing the apartment through the night and into the next day while obtaining a warrant to search the apartment).



the laptop, the hard drive, or the USB drive: not by formal motion in state or federal court and not by informal request of either the state or federal prosecutors. Indeed, Swartz did not even ask for a copy of the files stored on the equipment until the formal discovery process began much later in the state and federal court cases.

Where a property-owner fails to demand that officers return his equipment before they obtain a warrant, he cannot later argue that his possessory interests were harmed by a delay in obtaining a warrant. If Swartz needed the equipment back, he should have asked for its return at the time. See *United States v. Stabile*, 633 F.3d 219, 235-36 (3d Cir. 2011), cert. denied, 132 S. Ct. 399 (2011) (holding that three-month delay between seizure and obtaining a warrant to search hard drives not unreasonable, based in significant part on the grounds that a defendant who does not request the return of his property cannot argue that pre-warrant delay adversely affected his Fourth Amendment rights) (citing *United States v. Johns*, 469 U.S. 478, 487 (1985)); *United States v. Ivers*, 430 Fed. App'x 573, 576, 2011 WL 1594652 at \*2 (9<sup>th</sup> Cir. April 28, 2011) (rejecting defendant's argument that the FBI violated Fed. R. Crim. P. 41 by taking more than 10 days to execute a search warrant, because "[t]o the extent that the government unlawfully deprived Ivers of his property, Ivers was not without recourse. He could have filed a motion to return property at any time. Fed. R. Crim. P. 41(g). He simply did not do so."); *United States v. Lowe*, 2011 WL 1831593 at \*3 (S.D. Tex. May 12, 2011) (distinguishing *Mitchell* in part on the ground that the defendant never asked for the return of the searched property before the search warrant was obtained and there was "therefore no reason to believe that the defendant's possessory interests in the cell phone were substantially interfered with."). Because Swartz did not ask the Government to return his equipment before the warrants issued,

under *Johns, Stabile, Ivers, and Lowe*, his motion to suppress for pre-warrant delay must be denied.

***D. Swartz's Possessory Interests in the Laptop and Hard Drive Were Attenuated Because He Left Them Unattended for Extended Periods on MIT Property and Didn't Request Their Return***

In the alternative, any delay in obtaining the warrants to search the laptop, hard drive and USB drive had no cognizable effect on Swartz's possessory interests, because those interests were highly attenuated even before the equipment was seized. After officers seize property, there is no strict time limit within which they must obtain a warrant to search it. Whether pre-warrant delay is unreasonable is decided case by case. "There is unfortunately no bright line past which a delay becomes unreasonable. Instead, the Supreme Court has dictated that courts must assess the reasonableness of a seizure by weighing the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." *Burgard*, 675 F.3d at 1033 (internal quotation marks and citations omitted).

In balancing the individual's interests in his property against the government's interests in an investigation, the Court must consider the nature of the individual's possessory interests. If the individual gave others access to that property, or left that property in others' hands, then his possessory interests are attenuated and a pre-warrant delay affects those interests much less. See *United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998) (holding delay not unreasonable because, in part, "seizure is necessarily less intrusive where the owner has relinquished control of the property to a third party as was the case here [stolen equipment sold to third-party and then returned to defendant via commercial carrier, from which the equipment was seized],” and

seizing the property would not effectively restrain the liberty interests of the person from whom the property was seized, as with the seizure of a traveler's luggage); *see also United States v. Vallimont*, 378 Fed. App'x 972, 2010 WL 1857361 at \*3-\*4 (11<sup>th</sup> Cir. May 11, 2010), *rehearing and rehearing en banc denied*, 408 Fed. App'x 346 (11<sup>th</sup> Cir. 2010) (table) (distinguishing *United States v. Mitchell*, 565 F.3d 1347 (11<sup>th</sup> Cir. 2009), to find that a 45-day delay was not unreasonable in part because the defendant had a diminished privacy interest in his computer after having revealed its contents to a third party who could freely access its contents).

For the better part of three months before the seizure of the laptop and hard drive in Building W20, Swartz had only a tenuous possessory interest in the tools of his electronic theft. Swartz left his laptop and a series of five hard drives for extended periods at a time (1) running a high-speed downloading program unattended, (2) on MIT's property, (3) from which they would likely be removed by MIT personnel if discovered, (4) under circumstances intended to conceal that the equipment belonged to him and consequently would prevent its return to him. Even when Swartz retrieved the equipment on January 6, he again left it at another MIT building and room accessible to third parties. The slender possessory interests Swartz did have in the equipment were further thinned when he never even asked to have it returned to him before the search warrants were issued. *See supra*. The minimal possessory interests Swartz had in the equipment under the circumstances were outweighed by the government's interests in investigation.

***E. The Secret Service, Which Obtained the Warrant, Was Not the Same Entity that Seized the Equipment***

In yet another aspect, Swartz's assertion that the Secret Service infringed his possessory interests by delaying in obtaining a search warrant does not quite fit this situation or his legal

theory. The Secret Service did not seize his laptop, hard drive, or USB drive on January 6, 2011: the Cambridge Police Department did. Nor did the Secret Service possess this equipment before obtaining the warrants: the Cambridge Police Department did. Thus, the United States did not affect Swartz's possessory interests in his equipment until it executed warrants.

For all the reasons given above, the Cambridge Police Department did not seize or hold onto the equipment impermissibly long. The Cambridge Police Department was supporting a valid investigation and prosecution by the Commonwealth. But if the Court disagrees, then Swartz cannot simply morph allegations that local police held evidence too long in a local prosecution into a claim that federal law enforcement officers did so in a subsequent federal case.

***F. The Delay Was Justified***

Finally, regardless of whether the interference with Swartz's possession was pegged to the Cambridge Police Department or to the Secret Service, the investigators had reason for the delay. Lengthy pre-warrant delays can be reasonable if the officers' other duties interceded and the officers took their duties on the present case seriously. *See Vallimont*, 378 Fed. App'x at 976 ("For example, a delay could be justified if the assistance of another law enforcement officer had been sought, or if some overriding circumstances arose, necessitating the diversion of law enforcement personnel to another case.") (internal quotation marks omitted) (citing *United States v. Mitchell*, 565 F.3d 1347, 1352-53 (11<sup>th</sup> Cir. 2009)); *see also Stabile*, 633 F.3d at 236 (allowing delay in part because of agent's unavailability).

Here, the police and federal investigators were called in to investigate a complex computer crime on January 4, 2011. Through good fortune, they identified the suspect on

January 6, 2011. They still needed, however, to investigate what Swartz did and how he did it. That involved identifying and debriefing witnesses, obtaining technical and specialized information from both MIT and JSTOR, consulting with experts, and learning the facts both to understand the facts well and how to explain them with clarity and accuracy in warrant applications. Given that some of the equipment had been in MIT's hands for months beforehand, that Swartz did not ask for its return, and that the officers already had probable cause to hold onto the pieces of equipment as physical evidence in and of themselves without regard for their contents, any pre-warrant delay was reasonable. Although the officers theoretically might have obtained a warrant more quickly, "police imperfection is not enough to warrant reversal [for delay in obtaining a warrant]. With the benefit of hindsight, courts 'can almost always imagine some alternative means by which the objectives of the police might have been accomplished,' but that does not necessarily mean that the police conduct was unreasonable." *Burgard*, 675 F.3d at 1034 (quoting *United States v. Sharpe*, 470 U.S. 675, 686-87 (1985)) (finding police's delay in obtaining a warrant not unreasonable because although the police might have been able to work more quickly, he did not completely abdicate work or fail to see the urgency of the task).

Here, the officers were sufficiently diligent.

**VII. CONCLUSION**

For the reasons given above, the Court should deny all of Swartz's motions to suppress evidence.

Respectfully submitted,

Carmen M. Ortiz  
United States Attorney

By: /s/ Scott L. Garland  
STEPHEN P. HEYMANN  
SCOTT L. GARLAND  
Assistant U.S. Attorneys

**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ Scott L. Garland  
SCOTT L. GARLAND  
Assistant United States Attorney

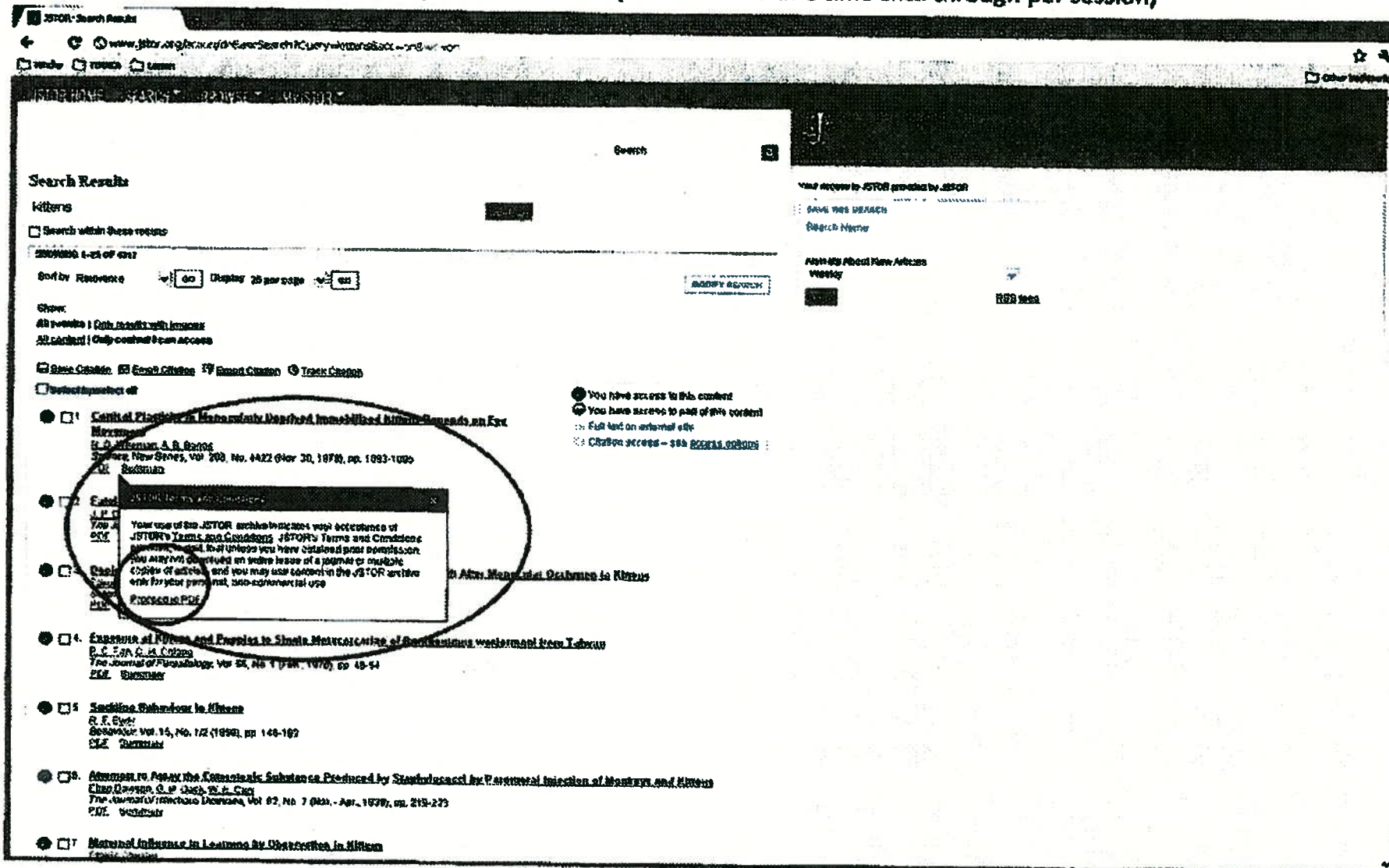
Date: November 16, 2012

**Defendant**

**Criminal No. 11-10260-NMG**

# EXHIBITS

Upon clicking the PDF link to obtain the article, the user is prompted with the Terms & Conditions overlay and must click Proceed to PDF in order to begin the download (note: this is a one time click through per session)







## CHICAGO JOURNALS

Review: [untitled]

Author(s): Jacqueline Long

Source: *Classical Philology*. Vol. 86, No. 4 (Oct., 1991), pp. 367-384

Published by: The University of Chicago Press

Stable URL: <http://www.jstor.org/stable/270097>

Accessed: 08/10/2010 12:41

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use 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.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=ucpress>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).



<http://www.jstor.org>

The University of Chicago Press is collaborating with JSTOR to digitize, preserve and extend access to *Classical Philology*.

### **The JSTOR Platform Terms and Conditions of Use**

The JSTOR Platform is a trusted digital repository providing for long-term preservation and access to leading academic journals and other scholarly materials from around the world. JSTOR is part of ITHAKA, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology, and is supported by libraries, scholarly societies, publishers, and foundations.

These Terms and Conditions of Use apply to individuals and institutions accessing content through JSTOR and, where applicable, are subject to the agreement entered into between JSTOR and a user's affiliated institution, such as a user's college or university. If you have questions about your affiliated institution's participation agreement with JSTOR, please contact your librarian.

Please note that these Terms and Conditions of Use may vary depending on the Collection or Content you are accessing and/or whether your institution is subject to grant-related project terms. *Please see Section 12 of these Terms and Conditions of Use for additional information.*

#### **1. Definitions:**

**"Authorized Users" means**

- (a) individuals who are affiliated with an Institutional Licensee, as defined below. This includes
  - (i) for educational non-profit and for-profit Institutional Licensees (such as colleges, universities, and secondary schools): currently enrolled students (including distance education students); on an ad hoc basis, researchers affiliated and/or visiting under the terms of an agreement with the Institutional Licensee; full and part-time staff; and on-site users physically present on the Institutional Licensee's premises ("Walk-In Users");
  - (ii) for museums; foundations; government agencies; corporate and for-profit organizations (other than for-profit educational organizations); and research center Institutional Licensees: full and part-time staff; on an ad hoc basis, researchers and lecturers affiliated and/or visiting under the terms of an agreement with the Institutional Licensee; and Walk-In Users;
  - (iii) for public library Institutional Licensees: full and part-time staff; Walk-In Users; and off-site users accessing the Licensed Content through a sessions-based arrangement entered into between JSTOR and the library;
- (b) individual members of scholarly societies that have entered into an agreement with JSTOR for access to specific Content via the JSTOR Platform ("Individual Access"); and
- (c) other users of specified content agreed upon in writing by or on behalf of JSTOR, including users of (i) Data for Research; (ii) the Publisher Sales Service (a service through which JSTOR facilitates users purchase of articles from publishers); and (iii) individual researchers not affiliated with a JSTOR participating institution, publication, or scholarly society.

**"Content" means** journal Back Issues and Current Issues, as defined in Sections 10.1 and 10.2, below, as well as portions of such journals, including articles and book reviews (each independently "Textual Content"); manuscripts and monographs (each independently also "Textual Content"); Data for Research (defined below); spatial/geographic information systems ("GIS") data; plant specimens ("Specimens"); and other materials made available by JSTOR.

"Data for Research" means data provided specifically for the purpose of textual extractions; describing and/or identifying content, usage, and operations; or cataloging information pertaining to the Content, to be used in research involving computational analysis rather than for purposes of understanding the intellectual meaning of such data.

"Institutional Licensee(s)" mean institution(s) that maintain(s) a valid Institutional Participation Agreement with JSTOR, available at <http://www.jstor.org/page/info/participate/new/forms.jsp>.

"JSTOR Platform" means JSTOR's integrated digital platform, which delivers and preserves Content and is aimed at furthering access to scholarly materials by the worldwide scholarly community.

"Licensed Content" means the Content for which an Authorized User's affiliated Institutional Licensee has entered into an Institutional Participation Agreement or other license agreement, or the Content available to an Authorized User through Individual Access, the Publisher Sales Service, or other programs. For more information about the JSTOR material licensed by your affiliated Institutional Licensee, please contact your librarian.

## **2. Use of the JSTOR Platform**

**2.1 Permitted Uses.** Institutional Licensees and/or Authorized Users may search, view, reproduce, display, download, print, perform, and distribute Licensed Content provided they abide by the restrictions in Sections 2.2 and elsewhere in these Terms and Conditions of Use, for the following Permitted Uses. Permitted Uses may be undertaken within the premises of an Authorized User's affiliated Institutional Licensee. Except in the case of Authorized Users who are Walk-In Users, Permitted Uses also may be undertaken remotely through secure access methods:

- (a) research activities;
- (b) classroom or organizational instruction and related classroom or organizational activities;
- (c) student assignments;
- (d) as part of a scholarly, cultural, educational, or organizational presentation or workshop, if such use conforms to the customary and usual practice in the field;
- (e) on an ad hoc basis and without commercial gain or in a manner that would substitute for direct access to the Content via services offered by JSTOR, sharing discrete Textual Content or Specimens with an individual who is not an Authorized User for purposes of collaboration, comment, or the scholarly exchange of ideas;
- (f) in research papers or dissertations, including reproductions of the dissertations, provided such reproductions are only for personal use, library deposit, and/or use solely within the institution(s) with which the Authorized User and/or his or her faculty readers are affiliated;
- (g) linking (see Section 2.3, below); and
- (h) Regarding Textual Content and Specimens, fair use under Section 107 of the U.S. Copyright Act, educational exceptions, or other similar provisions of the copyright laws or other intellectual property right laws in the United States or in other countries.

Should an Institutional Participation Agreement or other user agreement terminate or expire, the Institutional Licensee's affiliated Authorized Users or other Authorized Users may continue making use of Textual Content and/or Specimens that have been downloaded or printed out

providing such uses comply with these Terms and Conditions of Use, which shall survive the termination of access under the Institutional Participation Agreement or other user agreement.

**2.2 Prohibited Uses.** Institutions and users may not:

- (a) use or authorize the use of the JSTOR Platform or Content for commercial purposes or gains, including charging a fee-for-service for the use of JSTOR beyond reasonable printing or administrative costs. For purposes of clarification, "commercial purposes or gains" shall not include research whose end-use is commercial in nature;
- (b) except as set forth in Section 2.1(e) and 2.4, provide and/or authorize access to the Content available through Individual Access, the Publisher Sales Service, or other programs to persons or entities other than Authorized Users;
- (c) modify, obscure, or remove any copyright notice or other attribution included in the Content;
- (d) attempt to override, circumvent, or disable any encryption features or software protections employed in the JSTOR Platform;
- (e) Systematically print out or download Content to stock or replace print holdings;
- (f) undertake any activity that may burden JSTOR's server(s) such as computer programs that automatically download or export Content, commonly known as web robots, spiders, crawlers, wanderers or accelerators;
- (g) make any use, display, performance, reproduction, or distribution that exceeds or violates these Terms and Conditions of Use; or
- (h) incorporate Content into an unrestricted database or website, except that authors or other Content creators may incorporate their Content into such sites with prior permission from the publisher and other applicable rights holders;
- (i) download or print, or attempt to download or print: an entire issue or issues of journals or substantial portions of the entire run of a journal, other than on an isolated basis because of the relevance of the entire contents of a journal issue to a particular research purpose; or substantial portions of series of monographs or manuscripts; or
- (j) reproduce or distribute Content in bulk, such as by including Content in course packs, electronic reserves, repositories, or organizational intranets (but see Section 2.3, below).

**2.3 Linking.** JSTOR encourages the use of links to facilitate access to the Content by Authorized Users and Institutional Licensees, including but not limited to links to online syllabi, bibliographies, and reading lists. All Content has a stable URL that can be found in the Browse and Search interfaces of JSTOR's website as well as on the Article Information page for each discrete Content item. Further information on establishing stable links to material in JSTOR may be obtained from User Support ([support@jstor.org](mailto:support@jstor.org)).

**2.4 Interlibrary Loan.** Institutional Licensees may wish to use the Content for the purpose of fulfilling occasional requests from other libraries, a practice commonly called Interlibrary Loan. Institutional Licensees may use Licensed Content that consists of Textual Content or Specimens for Interlibrary Loan provided that such use is not at a volume that would substitute for a subscription to the journal or participation in JSTOR by the receiving institution and is in accordance with United States or international copyright laws, guidelines, or conventions. By way of example, Institutional Licensees shall comply with the CONTU Guidelines, available at <http://www.cni.org/docs/infopols/CONTU.html>, unless the Institutional Licensee is subject to similar international guidelines or customary and usual practices regarding Interlibrary Loan. Transmission of Licensed Content that consists of Textual Content or Specimens from one library to another (but not directly to users) through post or fax, or secure electronic transmission, such as Ariel or its equivalent, may be used in Interlibrary Loan. To facilitate direct contact with publishers for the provision of Textual Content outside the allowable scope of Interlibrary Loan

or for other permissions, Publisher contact information is available at <http://www.jstor.org/action/showJournals?browseType=publisherInfoPage>.

### **3. Intellectual Property Rights**

**3.1 General Intellectual Property Rights.** The JSTOR Platform and any trademarks, issued patents and patent applications, copyrights and copyright registrations and applications, rights in ideas, designs, works of authorship, derivative works, and all other intellectual property rights (collectively, "Intellectual Property") relating to the JSTOR Platform and its participating libraries, universities, publishers, scholarly societies, and journals are proprietary to JSTOR or, as applicable, the aforementioned entities, subject to the rights of third parties. Institutional Licensees and Authorized Users' use of JSTOR implies no rights to Intellectual Property except for the limited rights set forth in these Terms and Condition of Use.

**3.2 Trademarks.** Neither JSTOR nor Institutional Licensee may use the other's name or trademark(s) and Institutional Licensees and users may not use the name or trademark(s) of the above-noted entities in a way likely to cause confusion as to the origin of goods or services, or to endorse or show affiliation with the other, except as specifically approved. Notwithstanding the foregoing, (i) JSTOR may use Institutional Licensees' names and/or the names of their libraries in brochures or other materials to identify Institutional Licensees as participants in JSTOR along with other participants, and (ii) Institutional Licensees are encouraged to use JSTOR's name and logo to announce participation to Authorized Users and to train Authorized Users on the use of JSTOR.

**3.3 Use of Software.** JSTOR utilizes software and other electronic tools designed to permit Authorized Users to access, use, reproduce, display, and distribute Licensed Content ("Access Software"). Use of the Access Software and its related documentation is limited to the license granted herein. Institutional Licensees and users may not copy, distribute, modify, decompile, reverse engineer, circumvent, override or disable encryptions or other protections in, or create derivative works from the Access Software.

### **Access, Support, and Security**

#### **4.1 Responsibilities of JSTOR**

**4.1.1** JSTOR shall use reasonable efforts to provide continuous availability of the JSTOR Platform subject to periodic unavailability due to maintenance of the server(s), the installation or testing of software, the loading of journals as they become available, and downtime related to equipment or services outside the control of JSTOR, including public or private telecommunications services or internet nodes or facilities ("Maintenance Downtime"). If JSTOR fails to provide online availability to the JSTOR Platform for more than 72 hours during any period of 30 consecutive calendar days Institutional Licensee may, upon written request, (a) be granted its choice of a refund or a credit of a prorated portion of its annual access fee for each 30-day period so affected or (b) terminate its agreement by providing written notice to JSTOR.

**4.1.2** JSTOR shall provide support to Institutional Licensees and Authorized Users in accordance with the terms set forth at <http://www.jstor.org/page/info/about/policies/support.jsp>.

4.1.3 JSTOR is committed to supporting and working with industry standards and best practices for online information delivery as these standards are developed. In furtherance of this commitment, JSTOR shall use reasonable efforts to ensure that:

4.1.3.1 the JSTOR Platform is compliant with Section 508 of the Rehabilitation Act and W3C WAI Priority 1 accessibility standards. Further information about JSTOR and accessibility is available at <http://www.jstor.org/page/info/resources/librarians/accessibility.jsp>;

4.1.3.2 the JSTOR Platform meets ANSI/NISO z39.88-2004 OpenURL standards;

4.1.3.3 the JSTOR Platform is compatible with the NISO Metasearch XML Gateway (MXG) protocol in development, XML and SRU/SRW search interfaces; and

4.1.3.4 it makes available to Institutional Licensees COUNTER-compliant usage statistics.

4.1.4 Subject to constraints imposed by or in agreement with journal publishers, JSTOR shall use reasonable efforts to ensure that the journals contained in the JSTOR Platform are complete and faithful replications of the print versions of such journals.

#### 4.2 Responsibilities of Institutional Licensees

4.2.1 Institutional Licensees shall make reasonable efforts to ensure that access to the Licensed Content is limited to Authorized Users and to protect the Licensed Content from unpermitted use. Institutional Licensees shall notify JSTOR of any such unpermitted use of which they learn or are notified and shall cooperate with JSTOR in resolving problems of unpermitted use. In the event of violation of these Terms and Conditions of Use by an Authorized User, (a) JSTOR may suspend or terminate, or, where practicable, request that Institutional Licensee suspend or terminate, such Authorized User's access to the Licensed Content; (b) JSTOR may suspend or terminate the access of the Internet Protocol ("IP") address(es) or other authorization and authentication mechanisms from which such unauthorized use occurred; and/or (c) JSTOR may request Institutional Licensee to consider the imposition of further reasonable restrictions on access to, and downloading and printing from, the JSTOR Platform. JSTOR shall make reasonable efforts to contact the Institutional Licensee prior to any suspension or termination of access and to restore access promptly following successful resolution of the matter.

4.2.2 Access to the Platform shall be controlled by JSTOR through the use of IP addresses, Shibboleth, and/or, at JSTOR's sole discretion, passwords or other methods. Institutional Licensees shall be responsible for issuing and terminating passwords within its control, verifying the status of Authorized Users, providing lists of valid passwords or sets of IP addresses to JSTOR if applicable, and updating such lists on a regular basis.

4.2.3 The JSTOR Platform is intended to be accessible by telecommunications links between JSTOR's storage locations and Institutional Licensees' or Authorized Users' workstations or devices approved in advance in writing by JSTOR. Institutional Licensees and/or Authorized Users are responsible for establishing and maintaining hardware and Internet access to provide access to, and to transmit, the JSTOR Platform to Authorized Users. Institutional Licensees understand and agree that Internet browser software is required to access the JSTOR Platform. The Hardware and Software Requirements page available at <http://www.jstor.org/page/info/resources/librarians/tech.jsp#sysReqs> sets forth hardware

platforms and browsing software required and/or recommended for accessing the JSTOR Platform. Institutional Licensees and Authorized Users understand and agree that from time to time the Content may be added to or modified by JSTOR, that portions of the Content may migrate to other formats, and that the terms of the Hardware and Software Requirements page may be updated in a manner consistent with evolving industry standards. Institutional Licensees and Authorized Users shall be responsible for all costs associated with the use of and with establishing access to the JSTOR Platform, including but not limited to any telecommunications or other charges imposed by carriers, proprietary network operators and Internet access providers, or licenses for browser software, if any, as well as for all costs associated with printing from the JSTOR Platform.

#### 4.3 Responsibilities of Authorized Users

4.3.1 Authorized Users are responsible for maintaining the confidentiality and security of their username and/or password (if such are provided), and for all usage or activity by them of JSTOR. Except as permitted in Section 2.1(e), Authorized Users may not provide access to JSTOR to anyone else, including by setting up an anonymous remailer for purposes of allowing access to JSTOR.

4.3.2 Authorized Users promptly shall notify JSTOR and, where application, their affiliated Institutional Licensee, of any known or suspected unauthorized use(s) of their account or JSTOR, or any known or suspected breach of security, including loss, theft, or unauthorized disclosure or use of their username, password, and/or IP address. Any use of JSTOR beyond the scope or in violation of these Terms and Conditions of Use, knowing use of any password or username of another, or any fraudulent, abusive, or otherwise illegal activity, may be grounds for termination of an Authorized User's account, or termination of access to JSTOR from their IP address, without notice and at JSTOR's sole discretion.

#### 5. Warranty: Disclaimers

5.1 Authorized Users recognize that JSTOR is an aggregator of third-party Content, not the creator of the Content. JSTOR represents and warrants under the laws of United States that to its knowledge use of the JSTOR Platform and Licensed Content by Authorized Users in accordance with the terms of this Agreement shall not infringe the copyright of any third party. The foregoing shall not apply, however, to modifications or derivative works of the Content created by Institutional Licensees, Authorized Users or by any third party, nor usage of the JSTOR Platform or Content by Institutional Licensees or Authorized Users in violation of these Terms and Conditions of Use. *Please note that the foregoing further shall not apply to certain Collections. See Section 12 below for additional information.*

5.2 JSTOR shall not be liable, and Institutional Licensees and Authorized Users agree that they shall not hold JSTOR liable for any loss, injury, claim, liability, damages, costs, and/or attorneys fees of any kind that result from the unavailability of the JSTOR Platform or Content, delays or interruption of the services provided hereunder, or arising out of or in connection with Institutional Licensee's or Authorized Users' use of the JSTOR Platform or Content in violation of these Terms and Conditions of Use. If the JSTOR Platform fails to operate in conformance with the terms of this Agreement, Institutional Licensee shall immediately notify JSTOR, and, subject to Section 4.1.1 above, JSTOR's sole obligation shall be to repair the nonconformity. In no event shall JSTOR's liability to an Institutional Licensee exceed the fees paid to JSTOR by that Institutional Licensee for the term of the agreement then in effect.

**5.3 OTHER THAN ANY EXPRESS WARRANTIES STATED IN THIS SECTION 5, THE JSTOR PLATFORM, CONTENT, AND ACCESS SOFTWARE ARE PROVIDED ON AN "AS IS" BASIS, AND JSTOR AND ANY AND ALL THIRD PARTY CONTENT AND SOFTWARE PROVIDERS AND/OR LICENSORS ("CONTENT PROVIDERS") DISCLAIM ANY AND ALL OTHER WARRANTIES, CONDITIONS, OR REPRESENTATIONS OF ANY KIND (EXPRESS, IMPLIED, ORAL, OR WRITTEN) RELATING TO JSTOR, CONTENT, ACCESS SOFTWARE, OR ANY PARTS THEREOF, INCLUDING WITHOUT LIMITATION, ANY AND ALL IMPLIED WARRANTIES OF QUALITY, PERFORMANCE, COMPATIBILITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. JSTOR AND ALL CONTENT PROVIDERS MAKE NO WARRANTIES WITH RESPECT TO ANY HARM THAT MAY BE CAUSED BY THE TRANSMISSION OF A COMPUTER VIRUS, WORM, TIME BOMB, LOGIC BOMB, OR OTHER SUCH COMPUTER PROGRAM, EXCEPT THAT JSTOR WILL EXERCISE A REASONABLE LEVEL OF CARE TO PREVENT SUCH OCCURRENCES. JSTOR AND ALL CONTENT PROVIDERS FURTHER DISCLAIM ANY LIABILITY AND MAKE NO WARRANTIES WITH RESPECT TO ANY ERRORS OR OMISSIONS IN THE CONTENT, LIABILITY UNDER LIBEL LAWS, INFRINGEMENT OF RIGHTS OF PUBLICITY AND PRIVACY, MORAL RIGHTS, OR THE DISCLOSURE IN THE CONTENT OF CONFIDENTIAL INFORMATION AND FURTHER DISCLAIM ANY LIABILITY AND MAKE NO WARRANTY WITH RESPECT TO ANY CLAIMS AND/OR THREATENED CLAIMS (INCLUDING INTELLECTUAL PROPERTY RIGHTS CLAIMS AND/OR THREATENED CLAIMS) RELATING TO: LINKS BETWEEN THE JSTOR PLATFORM AND OTHER SITES AND/OR THE CONTENT ON SUCH LINKED SITES; ADAPTATIONS AND/OR MODIFICATIONS OF CONTENT; ANY AND ALL USES, REPRODUCTIONS, DISPLAYS, PERFORMANCES, AND DISTRIBUTIONS THAT EXCEED THE PERMITTED USES (WHETHER PERMITTED BY LAW OR OTHERWISE); AND/OR ANY USE(S), REPRODUCTIONS, DISPLAYS, PERFORMANCES, AND DISTRIBUTIONS MADE OF CONTENT (PRINTED OR EXPORTED) AFTER THE EXPIRATION OR TERMINATION OF THIS AGREEMENT AND/OR THE APPLICABLE INSTITUTIONAL PARTICIPATION AGREEMENT.**

**6. Withdrawing Content from JSTOR.** JSTOR may withdraw Content from JSTOR for good cause shown. JSTOR would endeavor, to the extent practicable, to minimize any inconvenience to Authorized Users caused by such withdrawal by, for example, seeking to withdraw Content only at the conclusion of an academic semester. However, should JSTOR be unable to avoid such inconvenience, JSTOR in no way shall be held liable for the withdrawal of such Content from the JSTOR Platform. If JSTOR withdraws a material amount of Content, Institutional Licensee may, upon written request, (a) be granted its choice of a refund or a credit of a prorated portion of its annual access fee for the Agreement then in effect or (b) terminate its agreement without penalty by providing written notice to JSTOR.

**7. Privacy Policy.** Use of JSTOR indicates acceptance of JSTOR's Privacy Policy, available at <http://www.jstor.org/page/info/about/policies/privacy.jsp> as it may be amended from time to time.

**8. Force Majeure.** Neither JSTOR nor Institutional Licensees or Authorized Users shall be liable for failures or delays in performing their obligations pursuant to this contract arising from any cause beyond their control, including but not limited to, act of God, acts of civil or military authority, terrorism, fires, strikes, lockouts or labour disputes, epidemics, wars, riots, earthquakes, storms, typhoons and floods and in the event of any such delay, the time for either party's



performance shall be extended for a period equal to the time lost by reason of the delay. If the conditions giving rise to the delay continue beyond thirty (30) consecutive days, either party may terminate its agreement with the other by giving written notice to the other party.

#### 9. General

9.1 These Terms and Conditions of Use are, where applicable, subject to and incorporated by reference into Institutional Licensees' Institutional Participation Agreements. In the event of any conflict between these Terms and Conditions of Use and the Institutional Participation Agreement applicable to an Institutional Licensee and/or Authorized User, the Institutional Participation Agreement shall prevail. Please contact your librarian for further details concerning your Institutional Participation Agreement, if you are affiliated with an Institutional Licensee. Information identifying Institutional Licensees is available at <http://www.jstor.org/page/info/about/organization/participantLists/participantsAll.jsp>.

9.2 These Terms and Conditions of Use shall be interpreted and construed according to United States Federal law, excluding any such laws or conventions that might direct the application of the laws of another jurisdiction, and venue shall lie exclusively in the federal and state courts of the United States, excluding any such laws to the contrary.

9.3 If any provision or provisions of these Terms and Conditions of Use shall be held to be invalid, illegal, unenforceable, or in conflict with the law of any jurisdiction, the validity, legality, and enforceability of the remaining provisions shall not be in any way affected or impaired thereby. A waiver of any breach of these Terms and Conditions of Use shall not be deemed a waiver of other breaches of these Terms and Conditions of Use.

9.4 The English language version of agreements with JSTOR shall be controlling over any other version.

9.5 These Terms and Conditions of Use are for the sole benefit of the parties to these Terms and Conditions of Use and are not intended for the benefit of any third party. The parties expressly disclaim the creation of any third party beneficiary rights under these Terms and Conditions of Use.

#### 10. Archiving and Post Cancellation Access

10.1 Archiving of Back Issues. As an archive serving the scholarly community, JSTOR provides long term preservation of the Back Issue material in its collections. Back Issue materials are journal volumes and issues dated behind the "Moving Wall" or older manuscripts and monographs. For further information about the Moving Wall, please see <http://www.jstor.org/page/info/about/archives/journals/movingWall.jsp>. Institutional Licensees typically pay two types of fees to JSTOR for Back Issue materials, an Annual Access Fee and an Archive Capital Fee. The Annual Access Fee is a periodic payment covering the Institutional Licensee's access to the JSTOR Platform. The Archive Capital Fee is one-time fee per JSTOR collection aimed at ensuring the long term preservation, upgrading, and enhancements of the scholarly materials in the JSTOR Platform. By paying the Archive Capital Fee to support a JSTOR collection, Institutional Licensees are securing reliable, long term preservation, upgrading, and enhancements of the Back Issue material in that collection for their institution. Should an Institutional Licensee elect to terminate access to a JSTOR Back Issue collection, it may resume access to that Back Issue collection and all content subsequently added to that

collection at any time in the future through payment of only the Annual Access Fee. It would not need to re-pay the Archive Capital Fee.

JSTOR recognizes that preserving scholarly material requires those entities responsible to employ best practices in preservation as well as to provide assurances about the security of the material and the organization's long term viability as a trusted archive. JSTOR pursues best practices and standards in the creation and maintenance of the JSTOR Platform, has established mirror sites and multiple back up files for all of the materials in the JSTOR Platform, and demonstrates its ability to provide continuing access on a daily basis. Additionally, for those Back Issue materials included in the JSTOR Platform that have print editions, JSTOR has established dedicated repositories at several participating institutions to house and preserve the print copies under archival-quality conditions. With the support of Institutional Licensees, JSTOR is also developing an endowment to ensure the long term operating viability of the JSTOR Platform.

**10.2 Post Cancellation Access:** Access to Current Issues shall be available to Institutional Licensees following the Institution's cancellation or non-renewal of a subscription to the Current Issues of the applicable journal ("Post Cancellation Access"). Current Issues materials are those issues of journal(s) published online back to the Digital Availability Date. The "Digital Availability Date" is the year when issues of the Journal(s) initially were published online in digital format, subject to exceptions as determined by the publisher and JSTOR. For purposes of clarification, the Digital Availability Date does not refer to when digitized versions of print issues became available as a JSTOR archival product but rather refers to when "born digital" versions of the title became available. Information concerning the Digital Availability Date for each title is available at <http://support.jstor.org/csp/titles/>. The scope of an Institution's Post Cancellation Access may include the following options:

- **Current Issues and Back Issues Content:** As noted in 10.1 above, institutions that continue to license Back Issues for applicable fees, whether in connection with a single publication subscription or a collection subscription, are assured of Post-Cancellation Access to issues of the journal "behind" the Moving Wall, which will advance annually. In addition, JSTOR will honor access to subscribed Current Issues for cancelled or non-renewed Subscriptions until the Moving Wall catches up to the year in which the Subscription was cancelled or discontinued.
- **Through Portico:** All of the journals whose Current Issues are available on the JSTOR Platform are also part of the Portico digital preservation service, which may include Post Cancellation Access under the terms set forth in the Portico Journal Archive License Agreement. Institutions participating in Portico may use this mechanism for obtaining Post Cancellation Access to a cancelled Current Issues journal.
- **Per-Publication Post Cancellation Access:** For Licensed Institutions for which neither of the above Post Cancellation options applies, JSTOR will provide Post Cancellation Access to subscribed Current Issues content for a small annual fee.

**11. Terms and Conditions Subject to Change.** In the interest of managing the evolving needs of Institutional Licensees, Authorized Users, and Content providers, JSTOR reserves the right to modify these Terms and Conditions, or any aspect of JSTOR, at any time. The most updated Terms and Conditions of Use will be posted on the JSTOR website. JSTOR shall notify Institutional Licensees via email of material modifications. A modification shall become effective for an Institutional Licensee if it does not object in writing to JSTOR within 60 (sixty)

days from the time JSTOR emails notice of the modification. In the event of such an objection, the Institutional Licensee shall have the right to terminate the Agreement on 30 (thirty) days written notice.

12. Additional Terms and Conditions of Use. Please see below for Terms and Conditions of Use specific to certain Collections or Content:

12.1 Institutions in the United Kingdom and Republic of Ireland, and their users please see [http://www.jisc-collections.ac.uk/catalogue/ireland/resources/how\\_to\\_subscribe](http://www.jisc-collections.ac.uk/catalogue/ireland/resources/how_to_subscribe) for The Ireland Collection.

12.2 Institutions in the United Kingdom and their users please see [http://www.jisc-collections.ac.uk/catalogue/19thc\\_pamphlets/how\\_to\\_subscribe](http://www.jisc-collections.ac.uk/catalogue/19thc_pamphlets/how_to_subscribe) for the 19<sup>th</sup> Century British Pamphlets Collection.

12.3 For the *African Plants, Cultural Heritage Sites and Landscapes*, and *Struggles for Freedom in South Africa* Collections, please see <http://www.jstor.org/page/info/about/policies/additionalTerms.jsp> addressing accessibility standards and Section 5.1 of these Terms and Conditions of Use.


12.4 For the *Current Scholarship Program*, please see <http://www.jstor.org/page/info/about/policies/csp.jsp> addressing Section 5.1 of these Terms and Conditions of Use.

Last Updated on July 1, 2010

MIT Network Dynamic Host Reg...

https://nic.mit.edu:444/bin/dynareg

Google



**Visitor Registration**

Please fill out the form below. You can use this registration for up to 14 days per year before you are required to formally register with us. If your registration expires and less than 14 days have been used, you will be diverted back to this form for an extension.

name:  Please do not include apostrophes

email:  limit of 32 characters

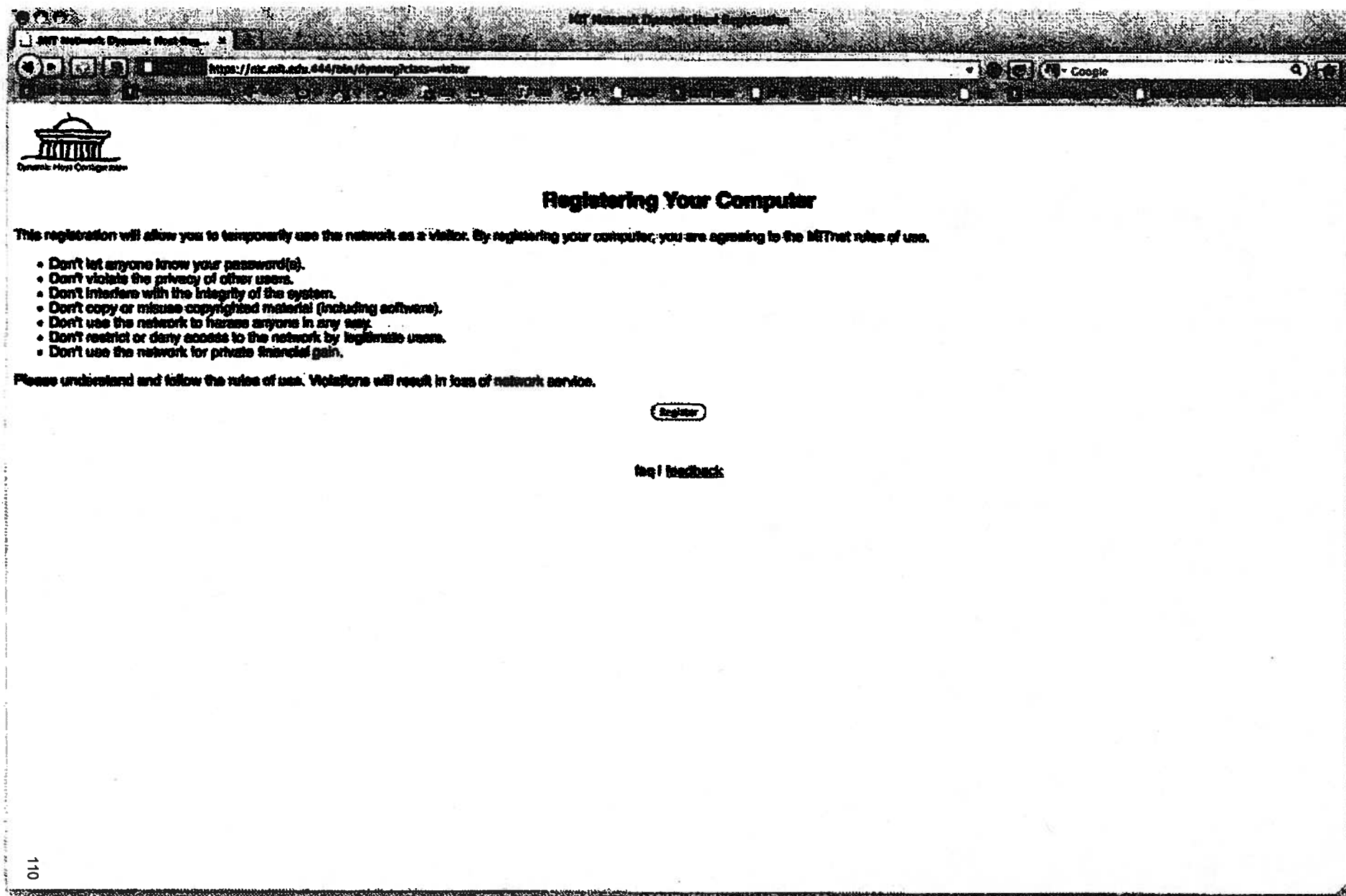
phone:

name of person/department you are visiting or event you are attending:

number of days (use 1 unless you know you will use the network for multiple consecutive days):

[faq](#) | [feedback](#)

109



For Faculty & Staff For Students For IT Support Providers



<input type="text"/>	Search
----------------------	--------

GET STARTED  
WITH IT

OUR  
SERVICES

SOFTWARE  
& HARDWARE

SECURE  
COMPUTING

ABOUT  
IS&T

## MITnet Rules of Use

### On this page:

[Overview](#)

[Summary](#)

[MITnet Rules of Use](#)

[Intended Use](#)

[Ethical Use](#)

[Proper Use](#)

### Overview

MITnet, MIT's campus-wide computer network, connects the MIT community and our guests to thousands of workstations, servers, printers, mobile devices and electronic resources of every kind located on and off campus. Network connectivity has many advantages which you will discover as you explore MITnet, and the Internet beyond. But connectivity also requires that users of the network understand their responsibilities in order to protect the integrity of the system and the privacy of other users.

This section summarizes the rules that apply to all users of MITnet. We expect you to follow all these rules, and we hope you will encourage others to follow them as well.

To report someone willfully violating the rules, send email to [stopit@mit.edu](mailto:stopit@mit.edu). If you believe you are in danger, call the Campus Police *immediately* at x3-1212.

### Summary

The listing below provides only summaries of the rules. For the full text of each rule, please see the following pages.

#### MITnet Rules of Use

##### *Comply with Intended Use of the System*

1. Don't violate the intended use of MITnet.

##### *Assure Ethical Use of the System*

2. Don't let anyone know your password(s).
3. Don't violate the privacy of other users.
4. Don't misuse the intellectual property of others.
5. Don't use MITnet to harass anyone in any way.

##### *Assure Proper Use of System Resources*

6. Don't misuse electronic communications and collaboration services.

#### MITnet Rules of Use

MITnet and other computing resources at MIT are shared among community members. The MITnet Rules of Use are intended to help members of the MIT community use MIT's computing and network facilities responsibly, safely, and efficiently, thereby maximizing the availability of these facilities to community members. Complying with them will help maximize access to these facilities, and assure that all use of them is responsible, legal, and respectful of privacy. If you have questions or wish further information about any of the MITnet policies outlined below, send email to [security@mit.edu](mailto:security@mit.edu).

***All network users are expected to follow these rules. Violations of the rules can subject the offender to institute disciplinary proceedings, loss of network privileges, and, in some cases, civil or criminal prosecution.***

**NOTE:** Laws that apply in "the real world" also apply in the "virtual" networked computer world (including MITnet). Laws about libel, harassment, privacy, copyright, stealing, threats, etc. are *not* suspended for computer users, but apply to all members of society whatever medium they happen to be using: face-to-face, phone, or computer. Furthermore, law-enforcement officials are more computer-savvy than ever, and violations of the law in "Cyberspace" are vigorously prosecuted.

**2. Neither MIT Nor the Government Violated the Wiretap or Stored Communication Act By Collecting Non-Content Network Addressing, Routing and Switching Records**

As alternative bases for suppression, Swartz argues that MIT violated the Wiretap Act and that the Government and MIT both violated the Stored Communications Act.

**a. No Statutory Suppression Remedies**

These statutory arguments fail from the outset because even had MIT or the Government violated these acts, neither act contains a suppression remedy for this type of case. Under the Wiretap Act, Congress provided a suppression remedy for violations involving wire and oral communications, but not those involving electronic communications, which are at issue here.<sup>16</sup> See *United States v. Mariwether*, 917 F.2d 955, 960 (6th Cir. 1990); *United States v. Reed*, 575 F.3d 900, 915 (9th Cir. 2009); *United States v. Amanuel*, 615 F.3d 117, 125 (2d Cir. 2010). Meanwhile, Congress determined that suppression was inappropriate for violations of the Stored Communications Act under *all* circumstances. 18 U.S.C. § 2708; Wayne R. LaFare, Jerold H. Israel, Nancy J. King, and Orin S. Kerr, *Criminal Procedure* § 4.8(F) (3d ed. 2011) ("Importantly, the Stored Communications Act does not include a statutory suppression remedy for the unlawful acquisition or disclosure of records of the contents of communications, whether they are wire or electronic communications."). See also, e.g., *U.S. v. Perrine*, 518 F.3d at 1202; *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998).

With no suppression remedies, the motion to suppress must be denied.

---

<sup>16</sup> While wire and electronic communications may both be transmitted by wire, "wire communications" by definition convey a human voice, while "electronic communications" do not. See 18 U.S.C. § 2510 (1), (12), (18). None of the communications that Swartz seeks to suppress were spoken; all, accordingly, were electronic communications.



While you should feel free to let others know your username (this is the name by which you are known to the whole Internet user community), you should *never* let anyone know your account passwords. This includes even trusted friends, and computer system administrators (e.g., IS&T staff).

Giving someone else your password is like giving them a signed blank check, or your charge card. You should never do this, even to "lend" your account to them temporarily. Anyone who has your password can use your account, and whatever they do that affects the system will be traced back to your username -- if your username or account is used in an abusive or otherwise inappropriate manner, you can be held responsible.

In fact, there is never any reason to tell anyone your password: every MIT student, faculty member, or on-campus staff person who wants an account of his or her own can have one. And if your goal is permitting other users to read or write some of your files, there are always ways of doing this without giving away your password.

For information about how to manage the security of your account, including advice on how to choose a good password, see IS&T: Security and IT Security: Passwords.

### **3. Don't violate the privacy of other users.**

The Electronic Communications Privacy Act (18 USC 2510 *et seq.*, as amended) and other federal laws protect the privacy of users of wire and electronic communications.

The facilities of MITnet encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing (see, for example, sections 11.2, 11.3, and 13.2 of MIT's Policies and Procedures). Users must therefore supplement the system's security mechanisms by using the system in a manner that preserves the privacy of themselves and others.

As Section 11.1 of MIT's *Policies and Procedures* notes, "Invasions of privacy can take many forms, often inadvertent or well-intended." All users of MITnet should make sure that their actions don't violate the privacy of other users, if even unintentionally.

Some specific areas to watch for include the following:

- *Don't try to access the files or directories of another user without clear authorization from that user.* Typically, this authorization is signaled by the other user's setting file-access permissions to allow public or group reading of the files. If you are in doubt, ask the user.

- *Don't try to intercept or otherwise monitor any network communications not explicitly intended for you.* These include logins, e-mail, user-to-user dialog, and any other network traffic not explicitly intended for you.
- *Unless you understand how to protect private information on a computer system, don't use the system to store personal information about individuals which they would not normally disseminate freely about themselves (e.g., grades, address information, etc.)*
- *Don't make any personal information about individuals publicly available without their permission.* This includes both text and number data about the person (biographical information, phone numbers, etc.), as well as representations of the person (graphical images, video segments, sound bites, etc.) For instance, it is *not* appropriate to include a picture of someone on a World Wide Web page without that person's permission. (Depending on the source of the information or image, there may also be copyright issues involved; cf. Rule 4).
- *Don't create any shared programs that secretly collect information about their users.* Software on MITnet is subject to the same guidelines for protecting privacy as any other information-gathering project at the Institute. (This means, for example, that you may not collect information about individual users without their consent.)
- *Don't remotely log into (or otherwise use) any workstation or computer not designated explicitly for public logins over the network -- even if the configuration of the computer permits remote access -- unless you have explicit permission from the owner and the current user of that computer to log into that machine.*

#### **4. Don't misuse the intellectual property of others.**

MIT faculty, students, and staff produce and consume a vast amount of intellectual property, much of it in digital form, as part of our education and research missions. This includes materials covered by the patent, copyright, and trademark laws, as well as license or other contractual terms.

Members of the MIT community also avail themselves of a wide variety of entertainment content that is available on the Internet, most of which is protected by copyright or subject to other legal restrictions on use.

All users need to insure that their use of all these protected digital materials respects the rights of the owners.

Digital materials that may be covered by this rule, without limitation, are:

- Data
- E-books
- Games

- Journals and periodicals
- Logos
- Movies
- Music
- Photographs and other graphics
- Software
- Textbooks
- Television programs
- Other forms of video content

You should assume that all materials are subject to these legal protections, and may have some restrictions on use. Ease of access, downloading, sharing, etc. should not be interpreted as a license for use and re-distribution.

Of particular concern is the prevalence of peer-to-peer file sharing as a medium for the unauthorized exchange of copyrighted materials, including movies, music, games, and other software programs. As required by the Higher Education Opportunity Act, MIT has developed and implemented a written plan to effectively combat the unauthorized distribution of copyrighted materials by users of MIT's network. For more information, see Copyright at MIT.

**5. Don't use MITnet to harass anyone in any way.**

"Harassment," according to MIT's Policies and Procedures (Section 9.5), is defined as:

"...any conduct, verbal or physical, on or off campus, which has the intent or effect of unreasonably interfering with an individual or group's educational or work performance at MIT or that creates an intimidating, hostile or offensive educational, work or living environment.... Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group."

The Institute's harassment policy extends to the networked world. For example, sending email or other electronic messages which unreasonably interfere with anyone's education or work at MIT may constitute harassment and is in violation of the intended use of the system.

Any member of the MIT community who feels harassed is encouraged to seek assistance and resolution of the complaint. To report incidents of on-line harassment, send email to [abuse@mit.edu](mailto:abuse@mit.edu). If you believe you are in danger, call the Campus Police *immediately* at x3-1212.

## **Assuring Proper Use of the System**

MITnet's resources, as well as the resources MITnet gives you access to (e.g., computing facilities, email and calendaring services, instant messaging, wikis, the web), are powerful tools that provide maximum benefit to the entire MIT community when used reasonably and in manners consistent with the intended uses of those resources.

### **6. Don't misuse electronic communications and collaboration services.**

MIT provides electronic communications and collaboration services to members of the MIT community. These services include, but are not limited to, electronic mail, mailing lists, instant messaging, message boards, websites, wikis, blogs, social networking sites, forums, collaborative spaces, Voice over IP (VoIP) and video services.

Some members of the MIT community access similar, or additional, 3rd party services on the Internet.

Users of all such services have a responsibility to use these services properly and to respect the rights of others in their use of these services, and in accordance with published terms of service.

Users may not use these services in violation of any applicable law.

All relevant MIT policies apply to the use of these services, but in particular:

- Any use that might contribute to the creation of a hostile academic or work environment is prohibited,
  - Any commercial use not required for coursework, research or the conduct of MIT business is prohibited,
  - Any non-incidental personal use such as advertisements, solicitations or promotions is prohibited
- [Note: some services exist on campus that have been designed for buying, selling and exchanging items within the MIT community, and those are allowed].

MIT Senior Leadership has authorized certain individuals to send electronic mail to large groups such as all Faculty, all employees, all undergraduates, Class of 2012, etc, or to the entire MIT community. These lists are not open to posts from the community at large. Contact the owners of these lists for further information.

Users should understand a service's policies prior to use. Service operators and providers should, to the extent feasible, publish their terms of service.

Any content posted to a service that is inconsistent with these rules, as well as unsolicited mail from outside of MIT (e.g., SPAM), may be subject to automated interception, quarantine and disposal.

**RELATED PAGES AND HOW  
TO**

Athena Rules of Use

Athena Computing Environment

Athena User Accounts

Athena Consulting

Obtaining an Athena Workstation

The Athena Release

Massachusetts  
Institute of Technology

Information Services and Technology |  
617.253.1101  
Ask the Help Desk or contact the IS&T  
Webmasters.

---

**FOR FACULTY & STAFF**

---

**FOR STUDENTS**

---

**FOR VISITORS**

---

**FOR IS&T STAFF**

---

**FOLLOW US**

---

## Guerilla Open Access *Manifesto*

Information is power. But like all power, there are those who want to keep it for themselves. The world's entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of private corporations. Want to read the papers featuring the most famous results of the sciences? You'll need to send enormous amounts to publishers like Reed Elsevier. There are those struggling to change this. *The Open Access Movement* has fought valiantly to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet, under terms that allow anyone to access it. But even under the best scenarios, their work will only apply to things published in the future. Everything up until now will have been lost.

That is too high a price to pay. Forcing academics to pay money to read the work of their colleagues? Scanning entire libraries but only allowing the folks at Google to read them? Providing scientific articles to those at elite universities in the First World, but not to children in the Global South? It's outrageous and unacceptable.

"I agree," many say, "but what can we do? The companies hold the copyrights, they make enormous amounts of money by charging for access, and it's perfectly legal — there's nothing we can do to stop them." But there is something we can, something that's already being done: we can fight back.

Those with access to these resources — students, librarians, scientists — you have been given a privilege. You get to feed at this banquet of knowledge while the rest of the world is locked out. But you need not — indeed, morally, you cannot — keep this privilege for yourselves. You have a duty to share it with the world. And you have: trading passwords with colleagues, filling download requests for friends.

Meanwhile, those who have been locked out are not standing idly by. You have been sneaking through holes and climbing over fences, liberating the information locked up by the publishers and sharing them with your friends.

But all of this action goes on in the dark, hidden underground. It's called stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew. But sharing isn't immoral — it's a moral imperative. Only those blinded by greed would refuse to let a friend make a copy.

Large corporations, of course, are blinded by greed. The laws under which they operate require it — their shareholders would revolt at anything less. And the politicians they have bought off back them, passing laws giving them the exclusive power to decide who can make copies.

There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.

We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks. We need to fight for *Guerilla Open Access*.

With enough of us, around the world, we'll not just send a strong message opposing the privatization of knowledge — we'll make it a thing of the past. Will you join us?  
July 2008, Eremo, Italy



http://www.guerillaopenaccess.com

2 November  
22 Nov 11, 7:04TOP  
2009  
2011Page 11  
Page 7

## Guerilla Open Access Manifesto

Information is power. But like all power, there are those who want to keep it for themselves. The world's entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of giant corporations. Want to read the papers featuring the most famous results of the century? You'll need to spend enormous amounts to purchase the papers like Fred Sherman.

We are those struggling to change this. The Open Access Movement has fought valiantly to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet under terms that we can all access it. But even under the best scenarios, their work will only apply to things published in the future. Everything up until now will have been lost.

It is no high a price to pay. Paying academics to put money in read the work of their colleagues? Scanning entire libraries but only allow the folks at Google to read them? Providing scientific articles to those at elite universities in the First World but not to children in the Global South? It's outrageous and unacceptable.

Yes, many say "but what can we do?" The companies hold the copyrights. They make enormous amounts of money by charging for access, and it's perfectly legal - there's nothing we can do to stop them. But there is something we can do something that's already being done: we can fight back.

We wish access to these resources - students, librarians, scientists - you have been given a privilege. You get to read at the banquet of knowledge while the rest of the world is locked out. But you need not - indeed, you must - keep this privilege for yourselves. You have a duty to share it with the world. And you have trading passwords with colleagues, filling download requests for friends.

We hope, those who have been locked out are not standing still by. You have been peering through holes and climbing over fences, liberating the information locked up by the publishers and sharing them with your friends.

All of this action goes on in the dark, hidden underground. It's called stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew. For sharing isn't immoral at all - it's necessary. Only those blinded by greed could refuse to let a friend make a copy.

Big corporations, of course, are blinded by greed. The laws under which they operate require it - their shareholders would revolt at anything less. And the politicians that have bought off back their passing laws giving them exclusive power to decide who can make copies.

It is no justice in following a strict law. It is time to come into the light and, in the great tradition of civil disobedience, declare our opposition to the private theft of public culture.

Need to make information, wherever it is stored, make our copies and share them with the world. We need to copy stuff that's out of copyright and add it to the archive. We need to have secret databases and put them on the Web. We need to download research journals and upload them to file sharing networks. We need to fight for Guerilla Open Access.

Enough of us around the world we do not just send a strong message opposing the privatization of knowledge - we'll make it a thing of the past. What you join us?

July 2008, Steven Ruby





## Host Lookup

### visitor registration

name:	Cary Host
email:	ghost@nrc.mil.edu
phone:	
days remaining:	9
last expiration date:	29-Sep-2010
MAC address:	8023547357b
status:	Inactive @inactive
comment: please include contact info	

record last updated by mhalet@nrc.mil.edu at Thu Sep 30 12:57:48 2010 EDT

[Delete Host](#)
[Update Host](#)

[faq](#) | [feedback](#)

Activity in MITnet computer registration database

Fields:

mac\_status, account, birthday, contact, sex, type, sex, vet\_name, vet\_email, vet\_phone, vet\_sponsor, vet\_course, vet\_chen, vet\_total, vet\_courses, comment, created\_at, created\_by, modified\_at, modified\_by

Registration on Sept. 24:

INSERT INTO host\_less VALUES ('00235a735fb', 0, 'visitor', NULL, NULL, 0.0, 'Gary Host', 'ghost@mailinator.com', '', 'NULL', NULL, 5, '24-Sep-2010', '24-Sep-2010', '22:46:19', 0, '30-Sep-2010', '12:57:46', 182635)Wg

Registration on Oct. 2:

INSERT INTO host\_less VALUES ('00235a735fb', 0, 'visitor', NULL, NULL, 0.0, 'Gary Host', 'ghost42@mailinator.com', '', 'NULL', NULL, 10, '13-Oct-2010', '12-Oct-2010', '10:20:37', 0, '13-Oct-2010', '05:54:22', 182635)Wg

Registration on Oct. 8:

INSERT INTO host\_less VALUES ('001722cb074', 0, 'visitor', NULL, NULL, 0.0, 'Grace Host', 'ghost42@mailinator.com', '', 'NULL', NULL, 5, '13-Oct-2010', '10-Oct-2010', '10:45:57', 182635)Wg

Registration on Oct. 22:

INSERT INTO host\_less VALUES ('004ceda0e735', 1, 'visitor', NULL, NULL, NULL, NULL, 'Grace Host', 'ghost12@mailinator.com', '', 'NULL', NULL, 10, '11-Nov-2010', '22-Oct-2010', '21:39:30', 0, '06-Nov-2010', '22:12:19', 0)Wg

Registration on Nov. 28:

INSERT INTO host\_less VALUES ('004ceda0e735', 1, 'visitor', NULL, NULL, NULL, NULL, 'Grace Host', 'ghost42@mailinator.com', '', 'NULL', NULL, 2, '07-Jan-2011', '28-Nov-2010', '18:28:19', 0, '06-Jan-2011', '12:44:43', 0)Wg

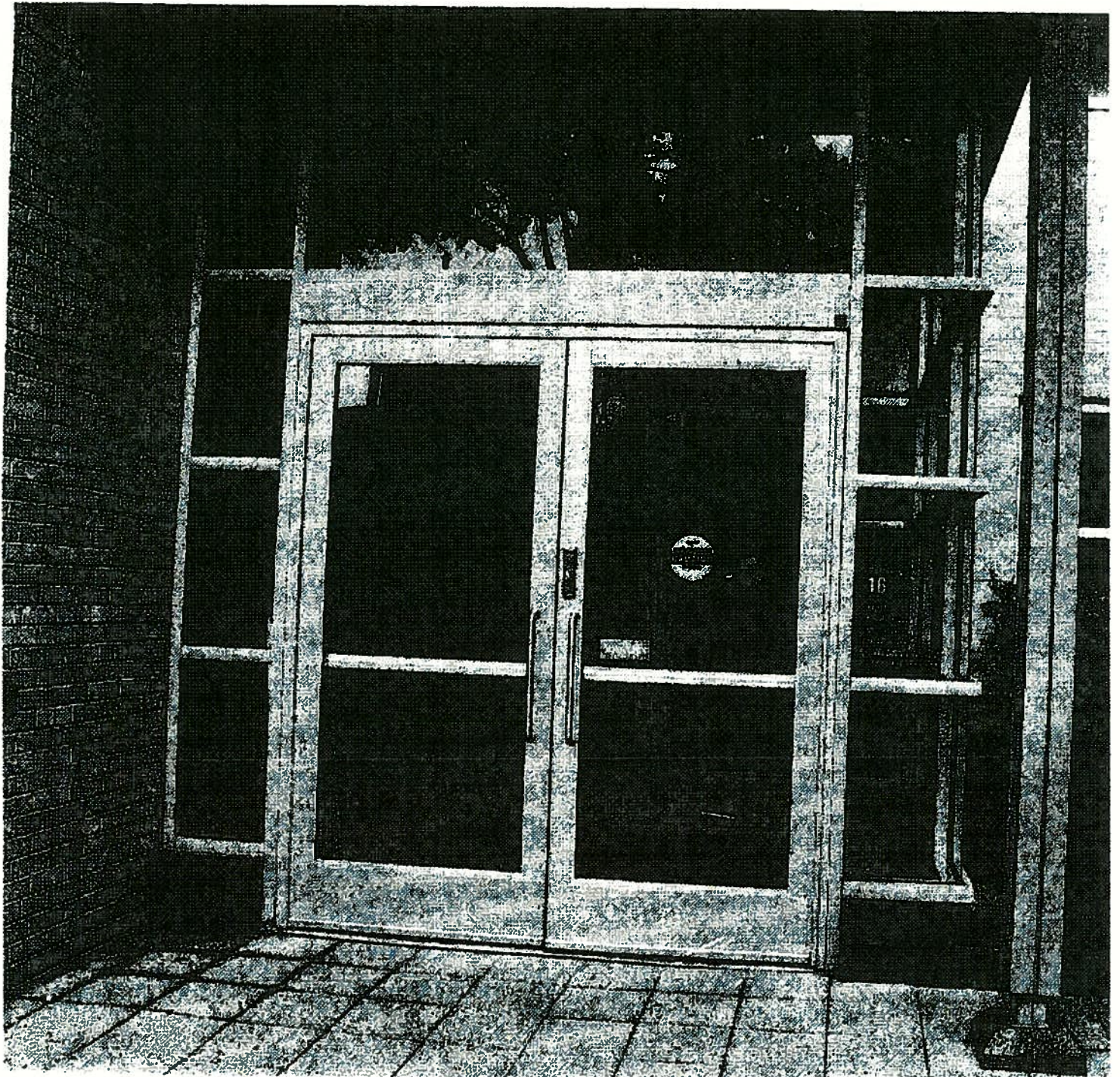
Activity in DHCP logs corresponding to computer registration database

ghost.bcdhcplogger/dhcp-20100925.gz-Sep 24 22:45:55 installer dhcpd: DHCP-OFFER on 10.2.55.247 to 00:23:5a:73:5fb (ghost-laptop) via 10.55.0.1

ghost.txd\dhcploggs\dhcp-20100930.gzSep 29 01:31:29 installer dhcpd: DHCP OFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20100930.gzSep 29 01:39:52 installer dhcpd: DHCP OFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101001.gzSep 30 18:11:25 installer dhcpd: DHCP OFFER on 18.2.55.247 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101003.gzOct 2 10:20:07 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101003.gzOct 2 10:20:50 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101003.gzOct 2 10:20:54 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101003.gzOct 2 10:26:44 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101003.gzOct 2 10:27:06 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101003.gzOct 2 10:27:52 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101003.gzOct 2 10:28:45 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101003.gzOct 2 10:29:29 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101003.gzOct 2 10:30:29 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101008.gzOct 7 01:49:06 installer dhcpd: DHCP OFFER on 18.2.55.166 to 00:17:42:2c:b0:74 (ghost-machbook) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101008.gzOct 8 22:12:09 installer dhcpd: DHCP OFFER on 18.2.55.166 to 00:17:42:2c:b0:74 (ghost-machbook) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101008.gzOct 8 22:15:06 installer dhcpd: DHCP OFFER on 18.2.55.166 to 00:17:42:2c:b0:74 (ghost-machbook) via 18.55.0.1  
ghost.txd\dhcploggs\dhcp-20101008.gzOct 8 22:58:57 installer dhcpd: DHCP OFFER on 18.2.55.212 to 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1  
ghost-laptop\_dhcp\_01062011.txtdhcp-20110107.gzJan 6 12:42:49 installer dhcpd: DHCP OFFER on 18.2.53.219 to 00:4c:ae:ad:c7:56 (ghost-laptop) via 18.53.0.1



RIF







126

# Building 16

M.I.T.

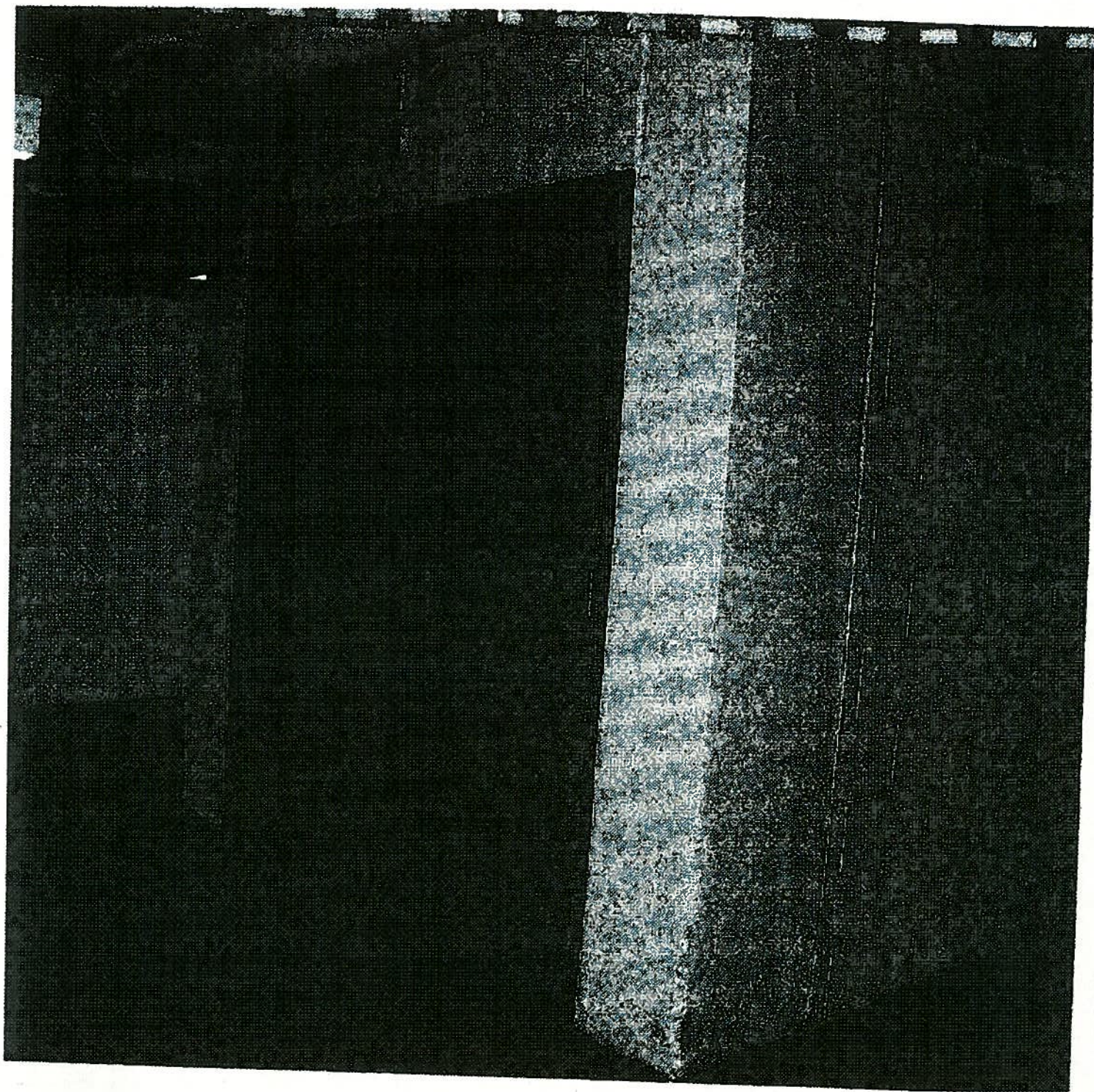
Private Property

No Trespassing

No Soliciting

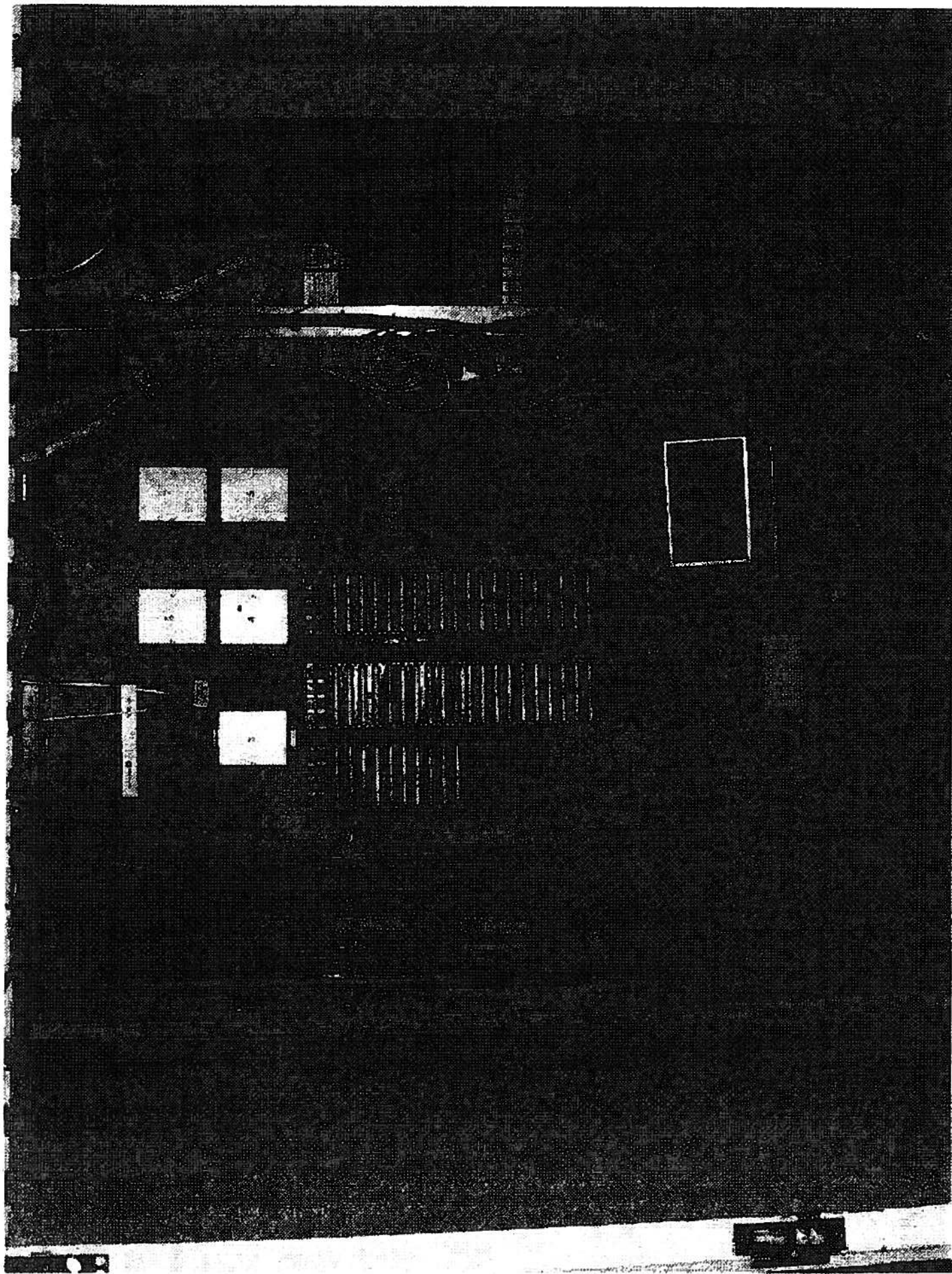
Trespassing and soliciting  
will be subject to prosecution

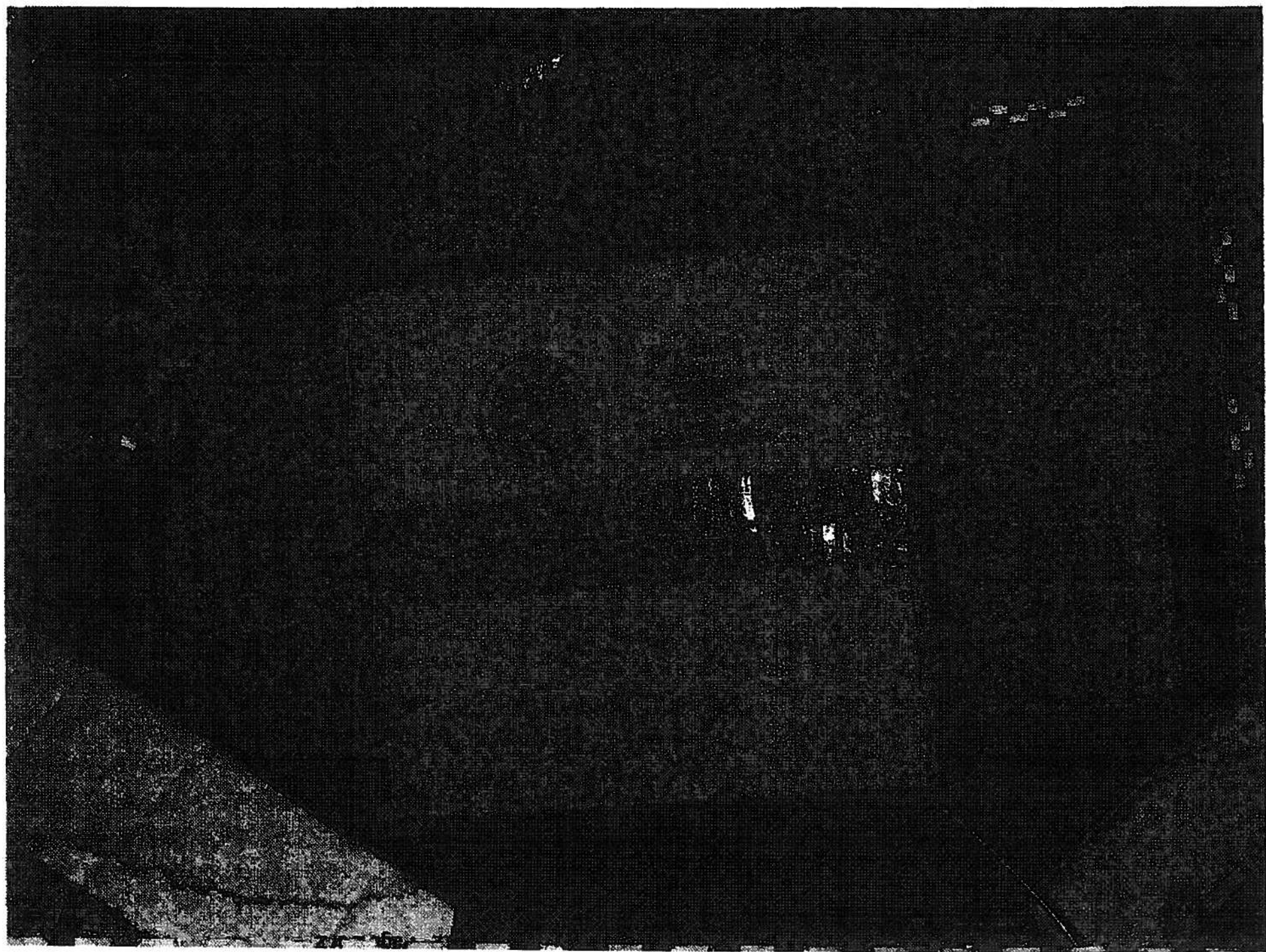




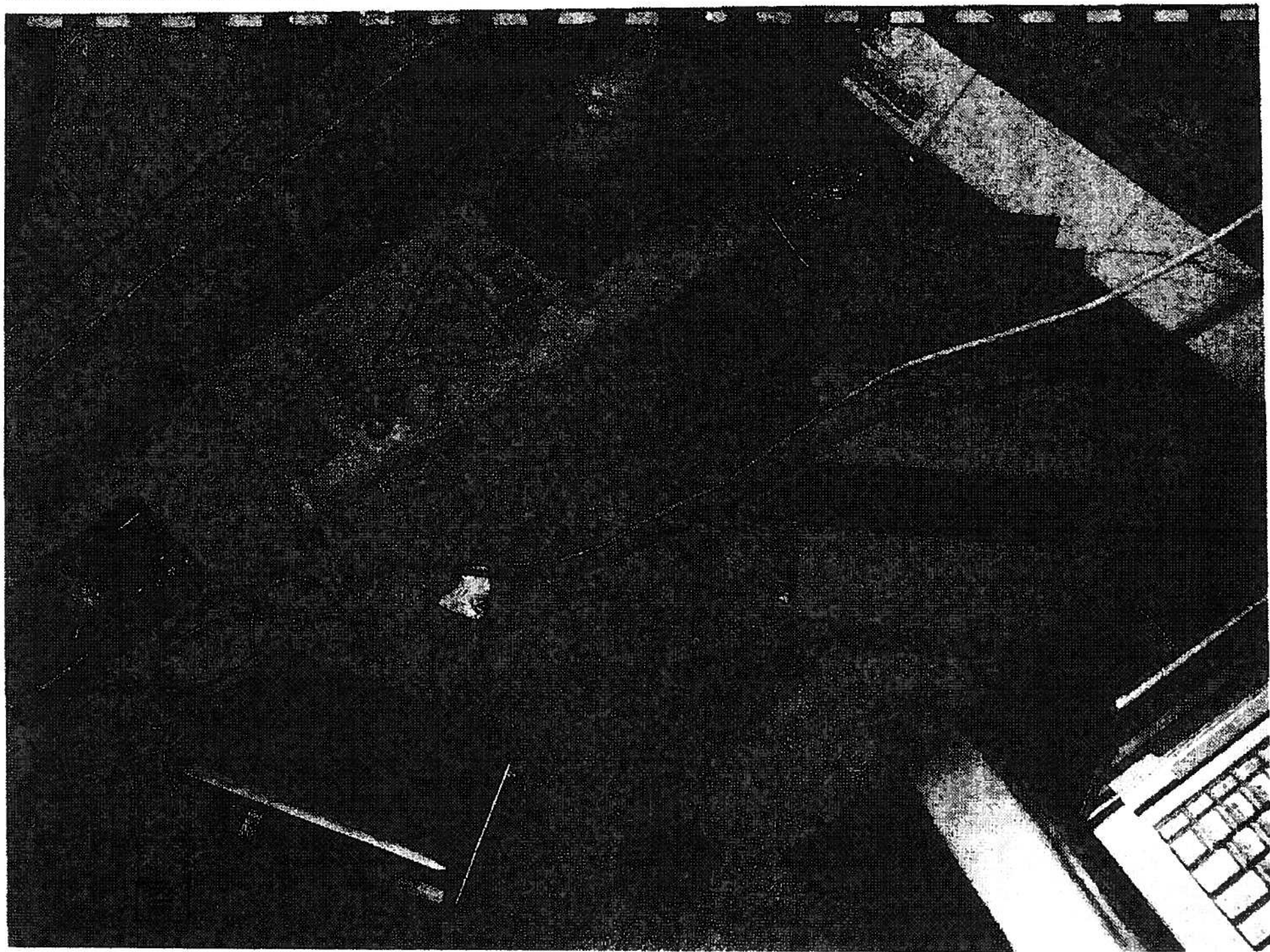
RIF

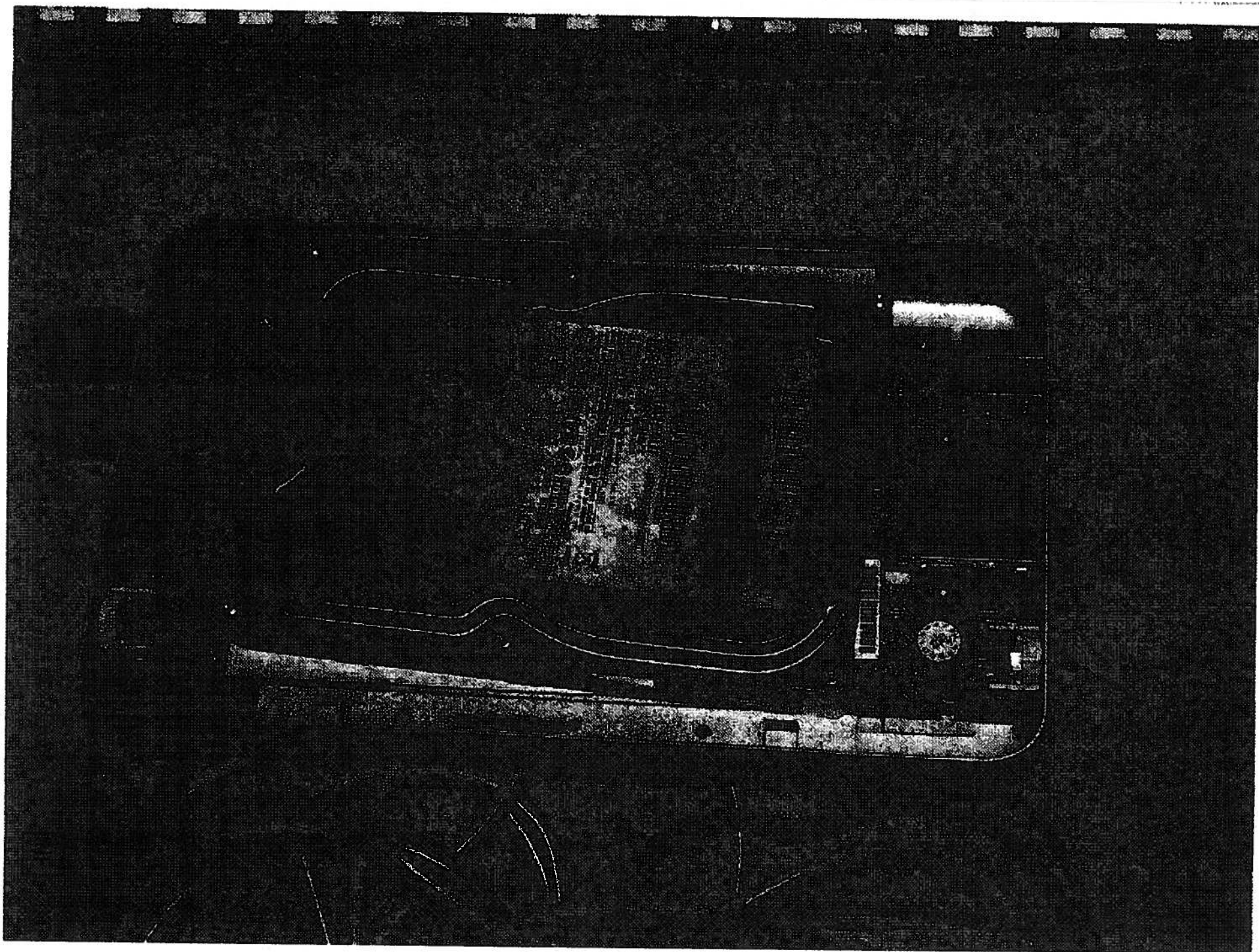








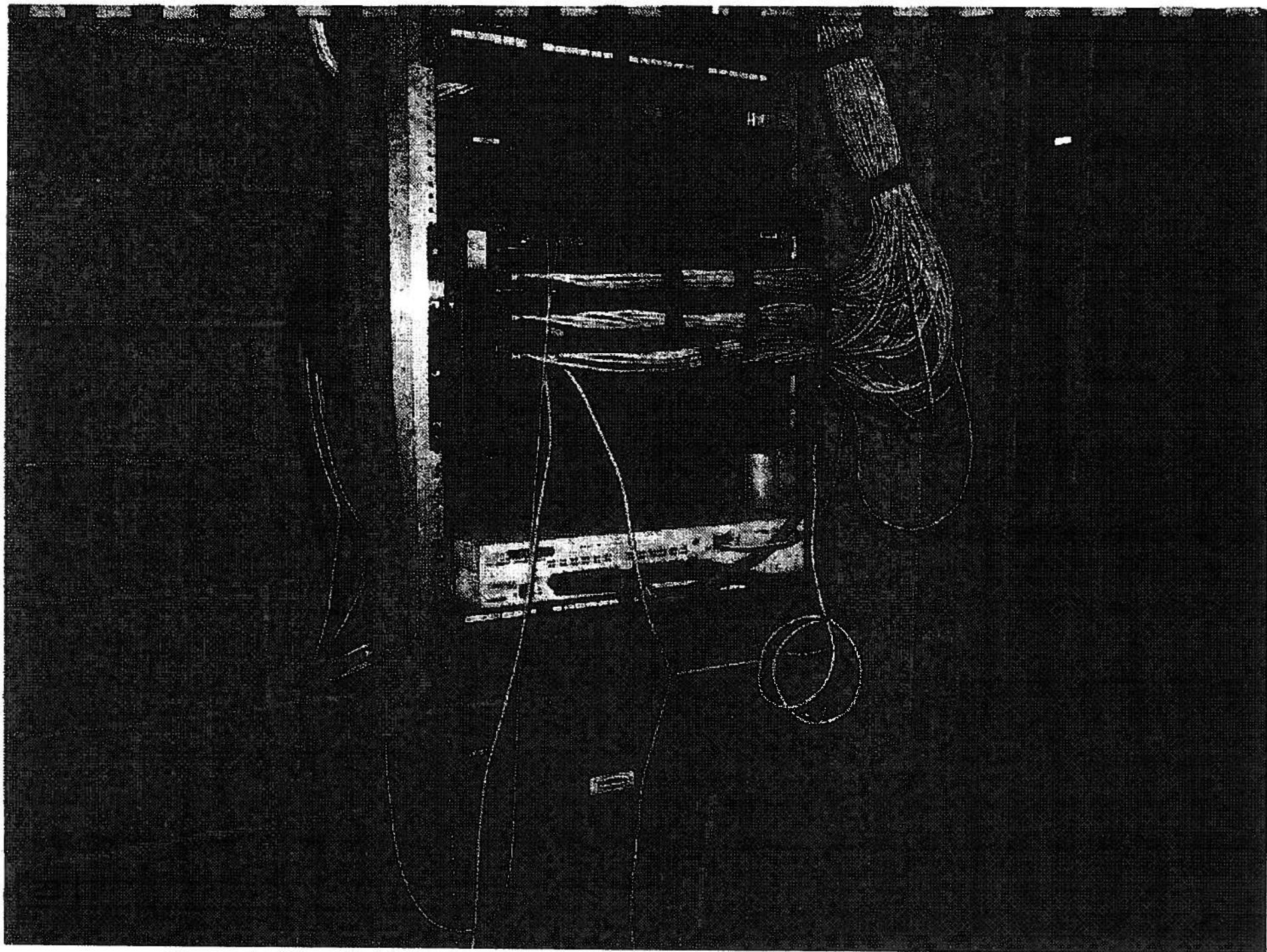


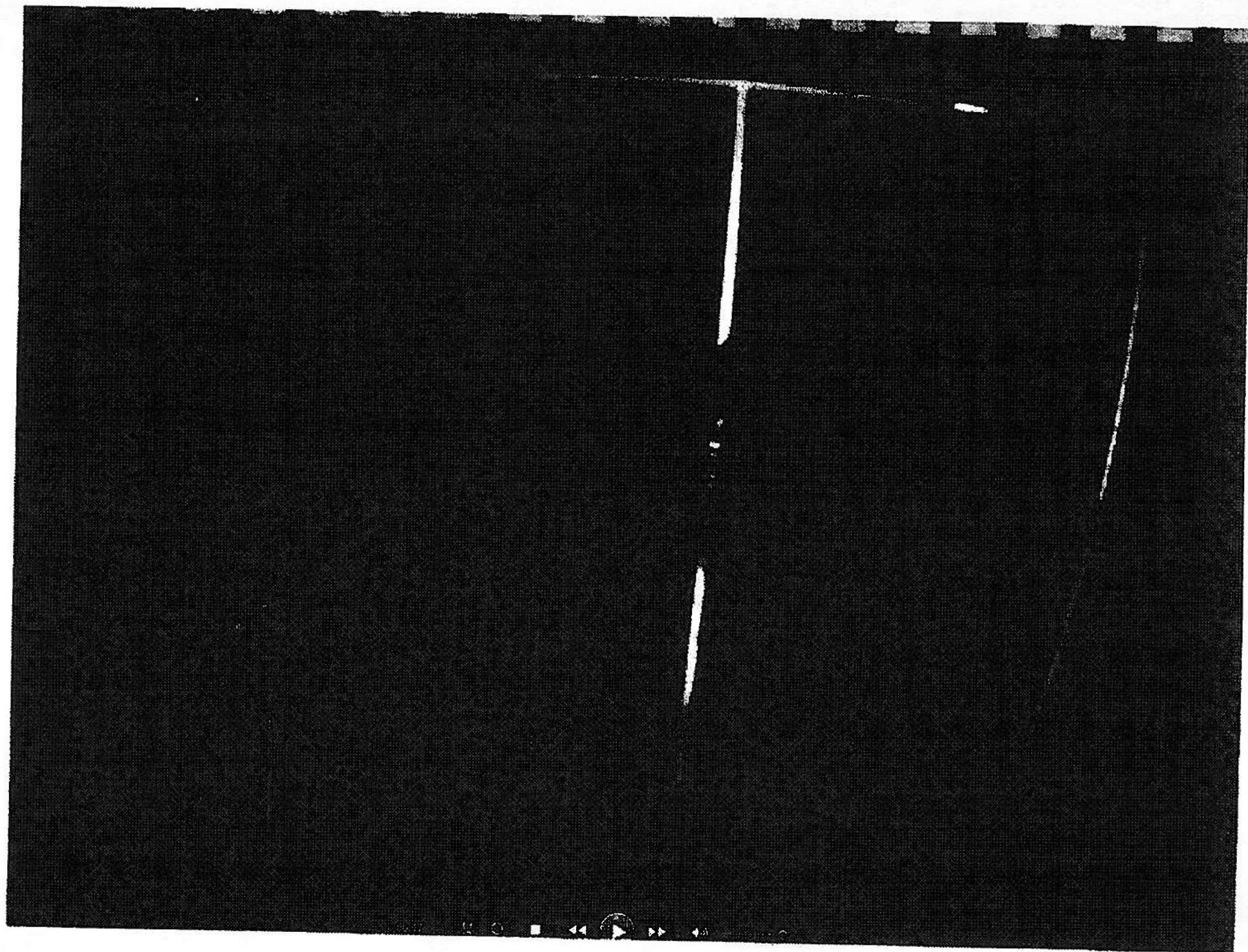




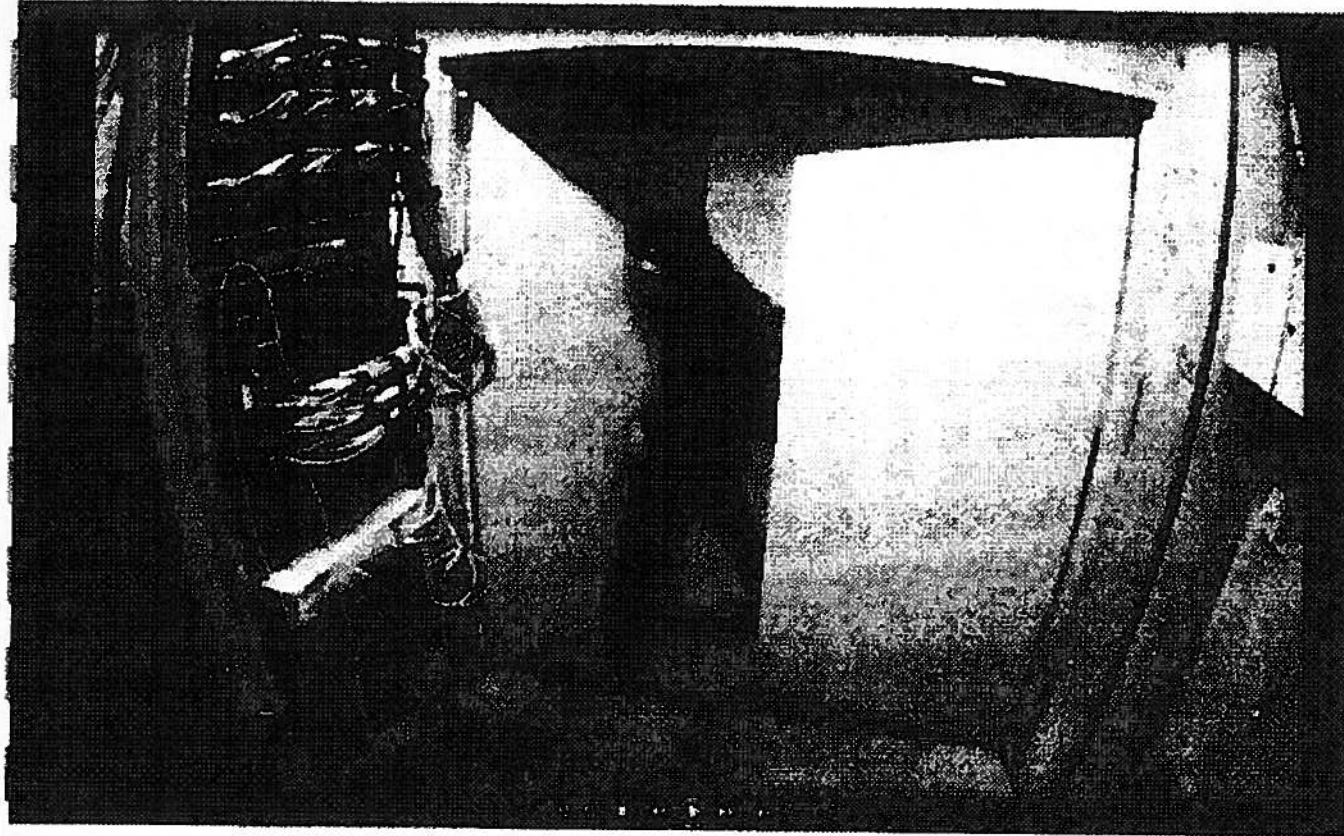
rocketfish.



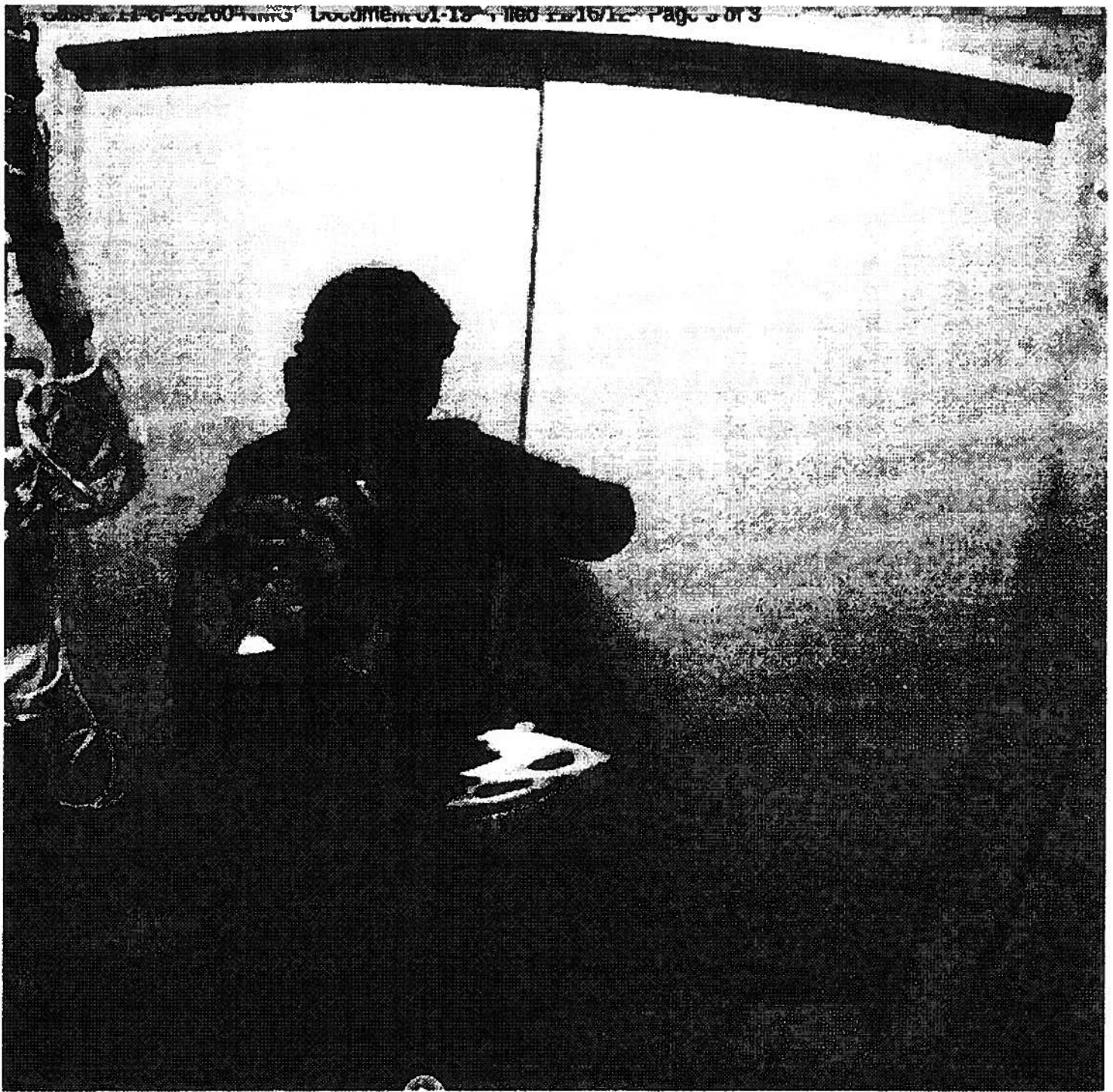








RIF



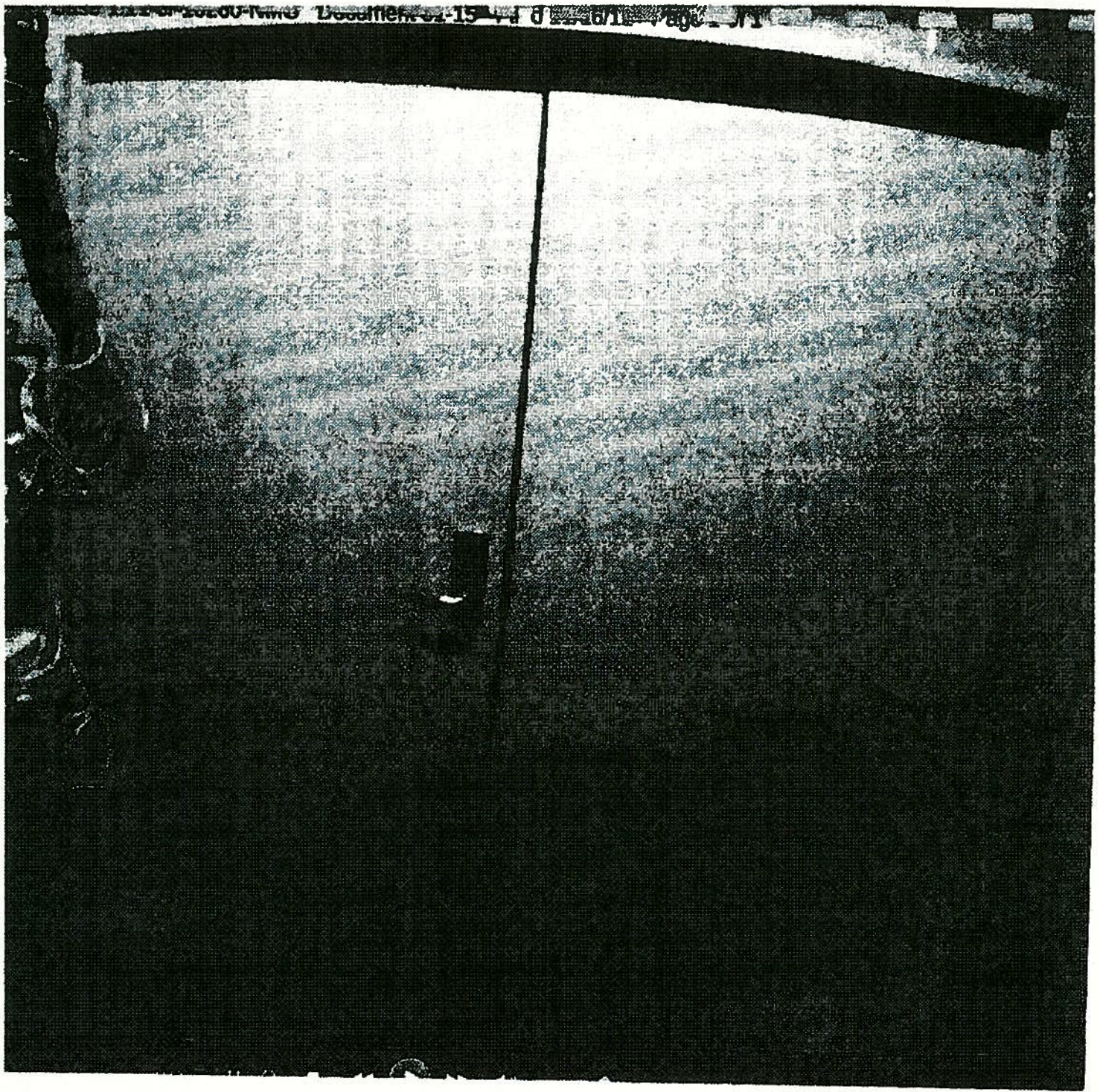
RIF





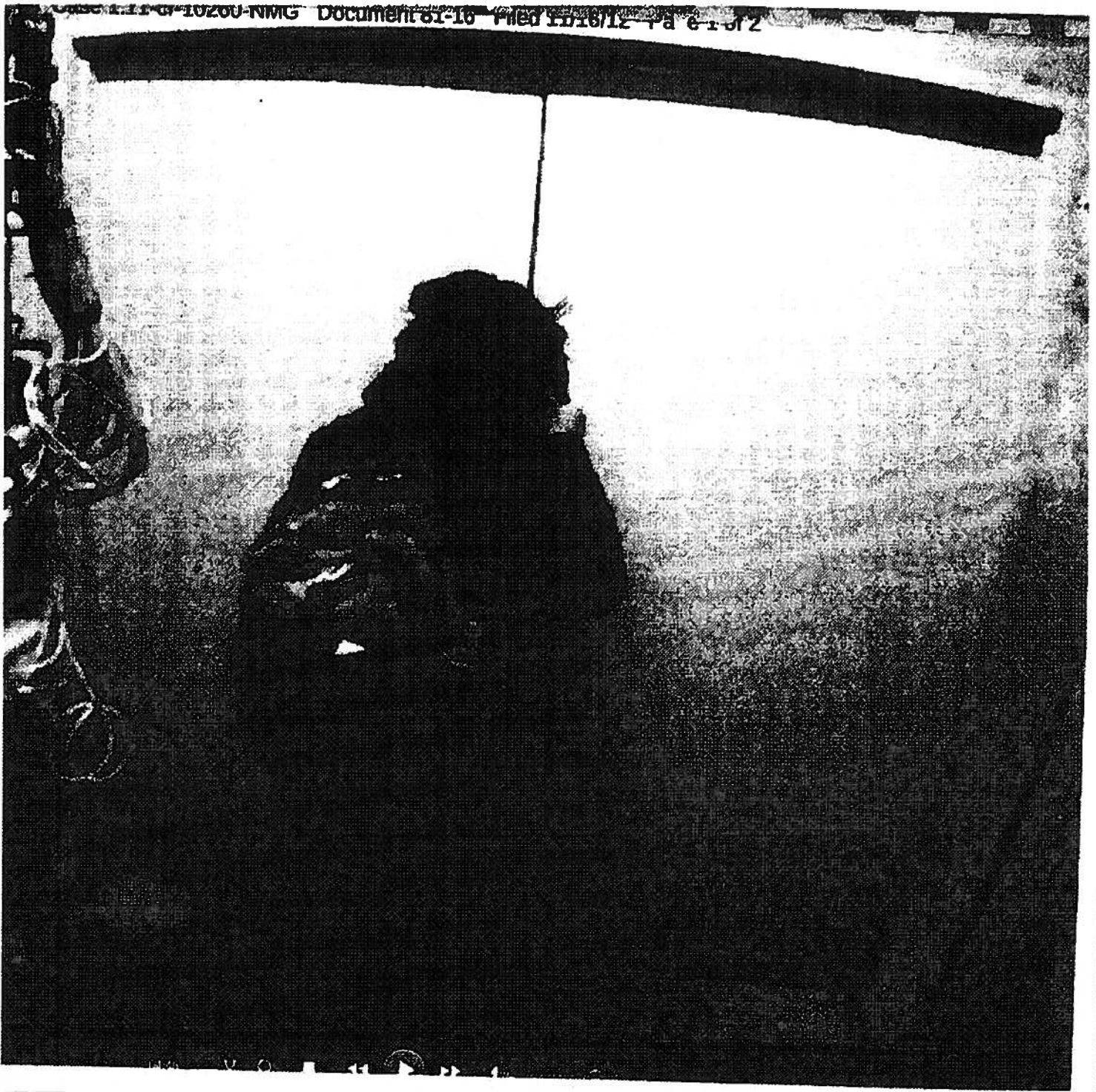
RIF





RIF





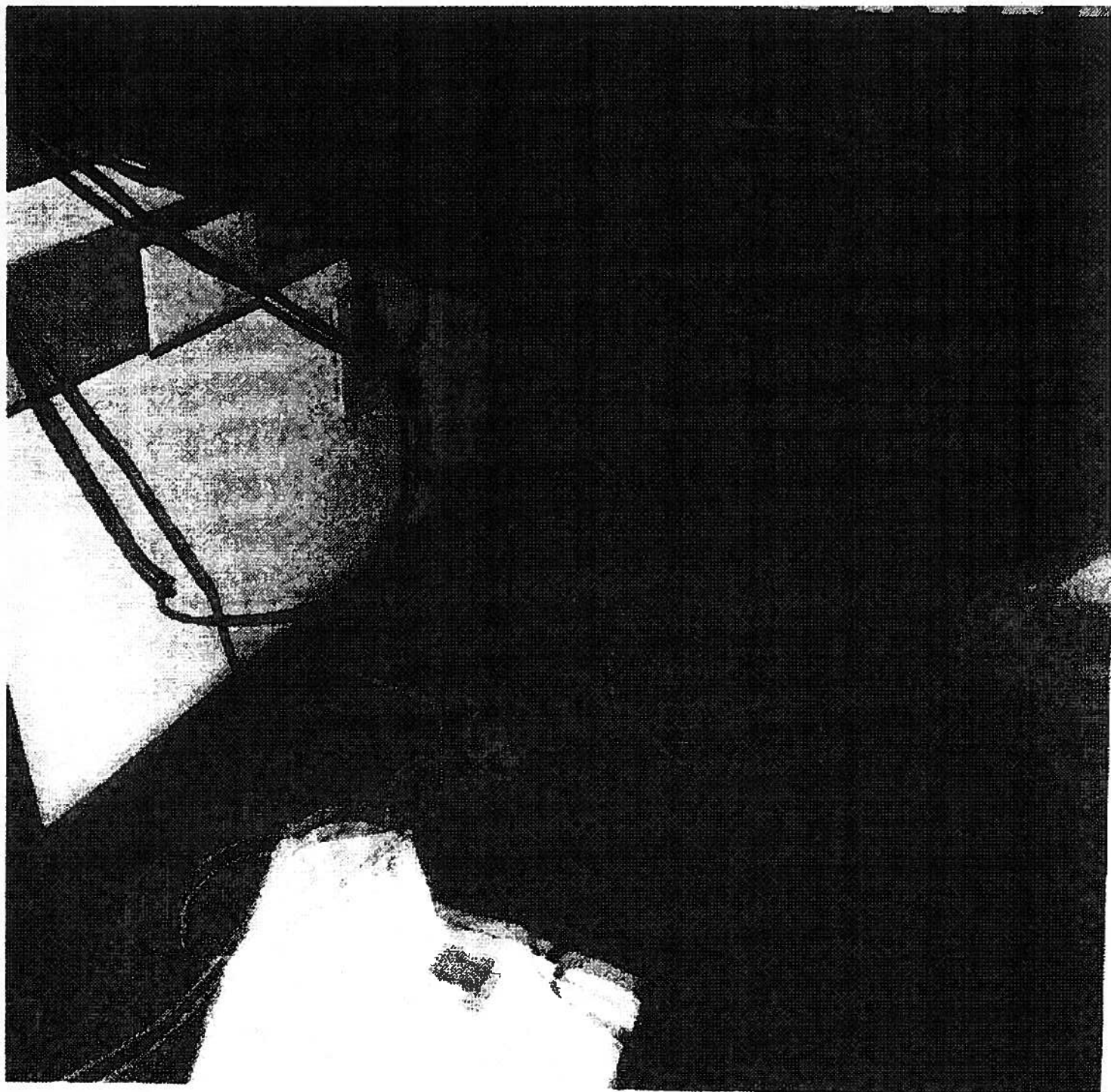
RIF





RIF





**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

**UNITED STATES OF AMERICA**

**v.**

**AARON SWARTZ,  
Defendant**

**Criminal No. 11-10260-NMG**

**PROTECTIVE ORDER**

Whereas the indictment in this case alleges that JSTOR and the Massachusetts Institute of Technology ("MIT") are victims of conduct committed by Defendant Aaron Swartz, and the materials discoverable in this case under Fed. R. Crim. P. 16 and L. R. 116.1-116.2 contain potentially sensitive, confidential and proprietary communications, documents, and records obtained from JSTOR and MIT, including discussion of the victims' computer systems and security measures,

The Court finds, without objection, good cause for entry of this Protective Order pursuant to Fed. R. Crim. P. 16(d):

1. The Government and the defense - that is, Defendant Swartz, his defense counsel and their staff, and any experts or investigators with whom defense counsel elects to consult - shall produce all documents, files and records discoverable under Fed. R. Crim. P. 16 and L.R. 116.1-116.2 ("discovery materials") for review in accordance with the conditions set by this Order.

2. With the exceptions listed below, the defense may obtain, make, and exchange amongst themselves copies of any discovery materials they deem necessary to prepare the defense of this case. All discovery materials and copies of discovery materials made by them or

provided to them by the Government shall be kept securely at their offices, residences, or while it is being reviewed in any other location

a. Per the parties' agreement, and without prejudice to a future application based on good cause by the defendant as set forth below, the Government will not, at this point, provide the defense complete imaged copies of all the files contained on four Samsung hard drives delivered to the Government by Defendant Aaron Swartz on June 17, 2011, and journal articles and other materials contained on a Maxtor hard drive seized by the Government at MIT on January 6, 2011. In lieu of the defense receiving complete copies of these hard drives:

i. The Government shall provide the defense electronic copies of those hard drives from which will be redacted all articles downloaded from JSTOR with the exception of approximately 350,000 separate articles that JSTOR released for free, public access on September 7, 2011, with those files' metadata intact in a form that will permit adequate forensic examination of the files. If this is not practicable, the parties shall work to agree on procedures to implement paragraph 2 (a) (v) (C) of this Order. The parties shall return to this Court with a proposed supplemental order and, if necessary, any disagreements they may have concerning sufficient security limitations carefully narrowed. All other aspects are severable and shall remain in full force and effect.

ii. The Government shall provide the defense a report listing all the files on the hard drives, along with the files' metadata.

iii. The Government shall provide the defense a bibliographic-type listing of the JSTOR articles found on the hard drives in sufficient detail to enable the defense to identify each such article.

iv. The Government shall make forensic copies of the complete unredacted hard drives available for review by the defense at the Boston Office of the Secret Service at reasonable times upon 7 day notice that any member of the defense wants to inspect or conduct forensic tests upon the hard drives. During any review conducted by the defense, the Secret Service shall make an agent otherwise unaffiliated with the investigation and prosecution of this case available to provide assistance. This agent shall not communicate with the prosecution team about what items the defense reviews and shall not be present during the viewing and/or testing, except at the defense's request or with prior approval of the Court. The parties will agree upon additional procedures necessary to ensure the security of the records and files stored on these hard drives in the event that the defense elects to do further inspection or conduct forensic examinations upon the hard drives at the Secret Service.

v. The defense shall not move for and the Court will not grant, an order requiring the Government to provide the defense copies of all the files on these hard drives, unless the defense demonstrates to the Court by a preponderance of the evidence that (A) defense counsel after inspection and forensic examination of the discovery materials provided pursuant to this agreement has a well founded basis, which will be particularized for the Court, that additional forensic testing on files other than those produced under subparagraph i, above, will lead to evidence material to the defense that cannot be adequately developed from the discovery materials provided pursuant to paragraphs 2 (a) (i-iii); or (B) the requested additional production is otherwise necessary to protect Defendant's constitutional rights; and (C) the defense's storage of and Defendant's access to all of these files will be under sufficiently secure restrictions to prevent the files' theft or public distribution (including restrictions on the location of the files'

storage, restrictions on who may have physical or electronic access to the files, the conditions under which Defendant can access the files, and the posting of substantial, third party financial security).

- b. Defendant may inspect, but may not be given or allowed to reproduce, copies of:
- (1) Two e-mail chains identified by the Government containing discussions of security weaknesses in MIT's computer network;
  - (2) Seven e-mail chains (or portions of chains) identified by the Government containing discussions of security methods of and weaknesses in JSTOR's network; and
  - (3) Police reports containing the name of one student who identified the defendant from a photo spread, and one non-law enforcement witness, who has been charged but not convicted in state court in a matter arising out of a personal relationship.

Defense counsel will, however, receive unredacted email chains and police reports of the identification which the defendant may fully inspect without copying at counsel's office.

3. The Government and the defense shall use the opposing party's discovery materials solely and exclusively to litigate this case (including investigation, pre-trial motions, trial preparation, trial, and appeal), and not for any other purpose. In the event either party believes it necessary to use any such materials for any other purpose, they may seek leave of Court, in which instance opposing counsel and victims shall have an opportunity to be heard.

4. Except when preparing a potential witness, the defense shall not show or make the discovery materials available by any means (electronic, physical or otherwise) to any person who is not a member of the defense, absent further order of this Court. Once a potential witness has also signed and agreed to be bound by the terms of this Protective Order, the defense may show



the potential witness discovery materials necessary to prepare them, but may not give or allow the potential witness to retain the discovery materials or copies of them.

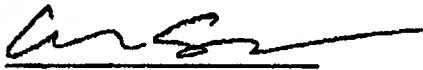
5. Each person receiving access to an opposing party's discovery materials other than counsel for the government, law enforcement officers, and counsel for the Defendant, shall first sign and date a copy of this Order to indicate their understanding of, acknowledgment of, and agreement to abide by its terms. Both the Government attorney and Defense counsel shall keep the signed copies in the event of a disclosure or use of discovery materials prohibited by this Order. Neither party shall be required to disclose to the other party who has been given access to what discovery materials, absent further order of this Court following an opportunity to be heard.

6. Defense counsel shall promptly notify the Government and this Court, and Government counsel shall promptly notify Defense counsel and this Court, if any discovery materials are (a) used in a manner inconsistent with this Order or (b) disclosed either intentionally or unintentionally to anyone not designated by this Order or further order of the Court. Each member of the defense and potential witness provided access to discovery materials shall promptly notify defense counsel of any such disclosures.

7. At the end of these proceedings, including any potential appeals, the defense shall destroy all copies of discovery materials received and made by it. Defense counsel may keep one copy of all discovery materials for such additional time as they deem necessary to ensure their ability to satisfy all professional obligations to Defendant in this matter. The Government may keep one copy of all defense discovery materials for such additional time as it deems necessary to satisfy its professional obligations and any relevant statutes, regulations, or policies.

B. Nothing in this protective order is intended to otherwise restrict the proper use by the parties of any discovery materials during the investigation, pre-trial litigation, trial preparation, trial or appeal of this matter.

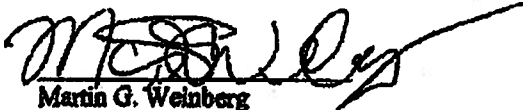
SO STIPULATED.



Aaron Swartz  
Defendant

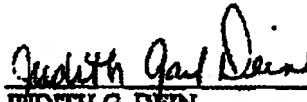


Stephen P. Heymann  
Scott L. Garland  
Assistant U.S. Attorneys



Martin G. Weinberg  
Defense Counsel

SO ORDERED.



JUDITH G. DEIN  
United States Chief Magistrate Judge

Date: 11/30/11

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS

----- x	
UNITED STATES OF AMERICA,	:
	:
Plaintiff,	:
	:
v.	:
	:
AARON SWARTZ,	:
	:
Defendant.	:
----- x	

Crim. No 11-CR-10260-NMG  
[PROPOSED] ORDER

WHEREAS the Estate of defendant Aaron Swartz ("the Estate") has moved to modify the protective order (Dkt. 28) in this case, a copy of which is appended hereto at Tab A for reference ("Protective Order"); and

WHEREAS non-parties Ithaca Harbors, Inc. d/b/a JSTOR ("JSTOR") and the Massachusetts Institute of Technology ("MIT") have been granted leave to intervene on the Estate's motion to modify the Protective Order, and the Estate and the United States have consented to the intervention; and

WHEREAS the Estate, the United States, JSTOR and MIT agree that the Protective Order should be modified to allow for public access to discovery materials in this case; and

WHEREAS on May 13, 2013, the Court issued a Memorandum & Order concerning the Estate's motion, granting the motions of JSTOR and MIT to intervene, resolving open issues as to the scope of redactions, and ordering the Estate, the United



States and the intervenors to submit a joint proposed order for modification of the Protective Order (the "Modification") consistent with that Memorandum & Order, which they submitted on May 31, 2013;

**IT IS HEREBY ORDERED THAT:**

1. The Protective Order is hereby modified, and discovery materials should be readied for public release, as follows:
  - a. For purposes of this Modification, the term "Discovery Documents" shall mean documents, electronic files, records and other materials the United States produced to the defendant Aaron Swartz, including the defendant's counsel (the "defendant") in this matter pursuant to Fed. R. Crim. P. 16 and this Court's Local Rules 116.1 and 116.2. The term includes all documents subject to the Protective Order. The term "Discovery Documents" shall also include any documents, electronic files, records and materials produced by JSTOR or MIT to the defendant pursuant to Fed. R. Crim. P. 17 or on any other basis.
  - b. Within five business days of this Order, the Estate and the counsel for the Estate shall deliver to the U.S. Attorney's Office in Boston ("USAO") the originals and all copies of all Discovery Documents, including all Discovery Documents in the possession of the Estate, counsel for the Estate, and/or the "defense" as that term is defined in ¶1 of the Protective Order, except for: (i) those Discovery Documents that have been destroyed pursuant to paragraph 2 of this Modification; and (ii) 2 sets of the Discovery Documents, which may be retained to perform the review process set forth in subparagraph 1(i) of this Modification.
  - c. The USAO shall remove from the Discovery Documents provided all documents that the counsel for the Estate and the USAO previously agreed should not be publicly disclosed, including without limitation (a) transcripts of grand jury testimony, (b) materials concerning immunity for grand jury witnesses, (c) the articles downloaded by Mr. Swartz from the JSTOR digital library (content and metadata), (d) any computer code that was used or intended to be used to download articles from JSTOR, and (e) criminal history information. Attached at Tab B is a more detailed description of the discovery materials not to be disclosed.
  - d. The USAO then may redact the remaining Discovery Documents to its reasonable satisfaction in order to remove the names of government employees, witnesses and potential witnesses (not otherwise employed by

JSTOR or MIT) and other information reasonably likely to facilitate the identification of such individuals, except for the names of the two Assistant United States Attorneys, three members of law enforcement and one expert witness that the USAO has previously agreed to leave unredacted. Redactions may include, but need not be limited to, names, email prefixes, personal e-mail suffixes, telephone numbers, home and work addresses, conference call numbers, Social Security numbers, birthdates, job titles, resumes, curriculum vitae, personnel files, and departments.

- e. The USAO then will provide the redacted set of Discovery Documents to MIT, at which time MIT may further redact the documents to its reasonable satisfaction in order to remove any references to possible network vulnerabilities and to the names of MIT employees, students, or other individuals affiliated with the Institute, and any other information reasonably likely to facilitate the identification of such individuals. Redactions may include, but need not be limited to, names, email prefixes, personal e-mail suffixes, telephone numbers, home and work addresses, conference call numbers, Social Security numbers, birthdates, job titles, resumes, curriculum vitae, personnel files, and departments.
- f. MIT then will provide the redacted set of Discovery Documents to JSTOR, at which time JSTOR may further redact the documents on the same terms set forth in the preceding subparagraph as to MIT.
- g. JSTOR then will provide the redacted set of Discovery Documents to the USAO for a final review, after which the USAO will distribute copies of the fully redacted set of Discovery Documents to the Estate, MIT and JSTOR. The USAO will affix new Bates numbering to this redacted set of Discovery Documents before distributing it.
- h. The USAO, MIT and JSTOR are directed to cooperate to generate the redacted set of Discovery Documents within 60 days of the USAO's receipt of the Discovery Documents from counsel for the Estate. If the 60 day period cannot be met, the parties affected by this document may seek leave of the Court to extend the period of time to complete the redaction process, which leave shall be granted for good cause shown.
- i. Upon receipt of the redacted set of Discovery Documents pursuant to subparagraph 1(g), above, the Estate shall have 14 days to review the proposed redactions and to serve the USAO, MIT and JSTOR with any written objections to the nature or extent of the redactions. Within 7 days following service of any such objections, the parties shall confer and attempt to resolve any disagreements. If the parties are unable to reach

agreement concerning any disputed redactions, the Estate may file a motion seeking resolution by the Court.

- j. Upon final agreement – or judicial resolution – concerning the scope of the redactions and completion of the redaction process (hereafter, “the Completion Date”), the resulting final redacted set of Discovery Documents (hereafter, “the Publicly Available Set of Documents”) shall be open to public inspection or distribution.

2. It is further ordered that:

- a. Within five business days of this Order, the Estate, counsel for the Estate, and the “defense” as that term is defined in ¶1 of the Protective Order, shall destroy all copies of the Discovery Documents not otherwise delivered to the USAO or permitted to be retained pursuant to ¶1(b) of this Modification, and shall certify to the Court that such destruction has occurred.
- b. If the Estate, counsel for the Estate or a member of the “defense” as that term is defined in ¶1 of the Protective Order has distributed any copies of the Discovery Documents to any person, or is otherwise aware that any person has possession of the Discovery Documents other than the United States, MIT or JSTOR, then, within five business days of this Order, the Estate, the counsel for the Estate or that member of the “defense” shall cause the destruction of those copies and certify to the Court that all such copies of the Discovery Documents have been destroyed, or, if the reasonable efforts of the counsel for the Estate do not result in causing the destruction of those copies, shall inform the Court of those individuals or entities who have copies of Discovery Documents that have not been destroyed and provide to the Court (with copies to MIT, JSTOR and the USAO) the signed copy of the protective order acknowledging receipt of the Protective Order and the agreement to be bound by it (as provided in ¶4 of the Protective Order).
- c. Within 5 business days of the Completion Date, the Estate, counsel for the Estate, and the “defense” as that term is defined in ¶1 of the Protective Order, shall destroy the 2 sets of the Discovery Documents whose retention is permitted by subparagraph 1(b) of this Modification, and shall certify to the Court that such destruction has occurred.
3. The Estate, counsel for the Estate, a member of the “defense” as that term is defined in paragraph 1 of the Protective Order, and/or any other person who they permitted to review or receive copies of the Discovery Documents shall not disclose any information contained in, or derived from, any material redacted in

the Publicly Available Set of Documents. For clarification, this prohibition includes but is not limited to, any public use, discussion, description or release of the information that is redacted in the Publicly Available Set of Documents.

4. No person who obtained access to the Discovery Documents in their unredacted form during the pendency of this criminal case (11-cr-10260-NMG), or thereafter, shall disclose any information contained in, or derived from, any material redacted in the Publicly Available Set of Documents. For clarification, this prohibition includes but is not limited to, any public use, discussion, description or release of the information that is redacted in the Publicly Available Set of Documents. For further clarification, nothing in this Order shall preclude JSTOR or MIT from voluntarily releasing documents from their own files.
5. If the USAO, MIT or JSTOR publicly releases its own documents with fewer redactions than will be contained in the Publicly Available Documents, nothing in Paragraphs 3 or 4 of this Modification prohibits anyone from discussing or commenting on the newly disclosed information.

SO ORDERED:

  
Hon. Nathaniel M. Gorton

6/3/13  
Dated

## **TAB A**



**TAB B**

**Discovery Materials Not to Be Disclosed**

1. Transcripts of witnesses' testimony before the state and federal grand juries which returned indictments against Aaron Swartz;
2. Documents and records pertaining to testimonial immunity accorded witnesses proffering and testifying;
3. Content and metadata downloaded from JSTOR between September 24, 2010 and January 6, 2011;
4. Police reports, criminal history reports, fingerprint identification reports, photospreads, booking photos, and booking reports pertaining to third parties;
5. Forensic images of computer hardware, all text reproductions of keepgrabbing.py, serveblocks.py, oaigrab.py and keepgrabbing2.py, and all section by section analyses of the listed computer code; and
6. Materials previously identified as containing sensitive network information produced subject to paragraph 2(b) of the Protective Order.

2197833.2  
2198026.1

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

**UNITED STATES OF AMERICA**

**v.**

**AARON SWARTZ,  
Defendant**

**Criminal No. 11-10260-NMG**

**PROTECTIVE ORDER**

Whereas the Indictment in this case alleges that JSTOR and the Massachusetts Institute of Technology ("MIT") are victims of conduct committed by Defendant Aaron Swartz, and the materials discoverable in this case under Fed. R. Crim. P. 16 and L. R. 116.1-116.2 contain potentially sensitive, confidential and proprietary communications, documents, and records obtained from JSTOR and MIT, including discussion of the victims' computer systems and security measures,

The Court finds, without objection, good cause for entry of this Protective Order pursuant to Fed. R. Crim. P. 16(d):

1. The Government and the defense - that is, Defendant Swartz, his defense counsel and their staff, and any experts or investigators with whom defense counsel elects to consult - shall produce all documents, files and records discoverable under Fed. R. Crim. P. 16 and L.R. 116.1-116.2 ("discovery materials") for review in accordance with the conditions set by this Order.

2. With the exceptions listed below, the defense may obtain, make, and exchange amongst themselves copies of any discovery materials they deem necessary to prepare the defense of this case. All discovery materials and copies of discovery materials made by them or

provided to them by the Government shall be kept securely at their offices, residences, or while it is being reviewed in any other location

a. Per the parties' agreement, and without prejudice to a future application based on good cause by the defendant as set forth below, the Government will not, at this point, provide the defense complete imaged copies of all the files contained on four Samsung hard drives delivered to the Government by Defendant Aaron Swartz on June 17, 2011, and journal articles and other materials contained on a Maxtor hard drive seized by the Government at MIT on January 6, 2011. In lieu of the defense receiving complete copies of these hard drives:

i. The Government shall provide the defense electronic copies of those hard drives from which will be redacted all articles downloaded from JSTOR with the exception of approximately 350,000 separate articles that JSTOR released for free, public access on September 7, 2011, with those files' metadata intact in a form that will permit adequate forensic examination of the files. If this is not practicable, the parties shall work to agree on procedures to implement paragraph 2 (a) (v) (C) of this Order. The parties shall return to this Court with a proposed supplemental order and, if necessary, any disagreements they may have concerning sufficient security limitations carefully narrowed. All other aspects are severable and shall remain in full force and effect.

ii. The Government shall provide the defense a report listing all the files on the hard drives, along with the files' metadata.

iii. The Government shall provide the defense a bibliographic-type listing of the JSTOR articles found on the hard drives in sufficient detail to enable the defense to identify each such article.

iv. The Government shall make forensic copies of the complete unredacted hard drives available for review by the defense at the Boston Office of the Secret Service at reasonable times upon 7 day notice that any member of the defense wants to inspect or conduct forensic tests upon the hard drives. During any review conducted by the defense, the Secret Service shall make an agent otherwise unaffiliated with the investigation and prosecution of this case available to provide assistance. This agent shall not communicate with the prosecution team about what items the defense reviews and shall not be present during the viewing and/or testing, except at the defense's request or with prior approval of the Court. The parties will agree upon additional procedures necessary to ensure the security of the records and files stored on these hard drives in the event that the defense elects to do further inspection or conduct forensic examinations upon the hard drives at the Secret Service.

v. The defense shall not move for and the Court will not grant, an order requiring the Government to provide the defense copies of all the files on these hard drives, unless the defense demonstrates to the Court by a preponderance of the evidence that (A) defense counsel after inspection and forensic examination of the discovery materials provided pursuant to this agreement has a well founded basis, which will be particularized for the Court, that additional forensic testing on files other than those produced under subparagraph i, above, will lead to evidence material to the defense that cannot be adequately developed from the discovery materials provided pursuant to paragraphs 2 (a) (i-iii); or (B) the requested additional production is otherwise necessary to protect Defendant's constitutional rights; and (C) the defense's storage of and Defendant's access to all of these files will be under sufficiently secure restrictions to prevent the files' theft or public distribution (including restrictions on the location of the files'

storage, restrictions on who may have physical or electronic access to the files, the conditions under which Defendant can access the files, and the posting of substantial, third party financial security).

- b. Defendant may inspect, but may not be given or allowed to reproduce, copies of:
  - (1) Two e-mail chains identified by the Government containing discussions of security weaknesses in MIT's computer network;
  - (2) Seven e-mail chains (or portions of chains) identified by the Government containing discussions of security methods of and weaknesses in JSTOR's network; and
  - (3) Police reports containing the name of one student who identified the defendant from a photo spread, and one non-law enforcement witness, who has been charged but not convicted in state court in a matter arising out of a personal relationship.

Defense counsel will, however, receive unredacted email chains and police reports of the identification which the defendant may fully inspect without copying at counsel's office.

3. The Government and the defense shall use the opposing party's discovery materials solely and exclusively to litigate this case (including investigation, pre-trial motions, trial preparation, trial, and appeal), and not for any other purpose. In the event either party believes it necessary to use any such materials for any other purpose, they may seek leave of Court, in which instance opposing counsel and victims shall have an opportunity to be heard.

4. Except when preparing a potential witness, the defense shall not show or make the discovery materials available by any means (electronic, physical or otherwise) to any person who is not a member of the defense, absent further order of this Court. Once a potential witness has also signed and agreed to be bound by the terms of this Protective Order, the defense may show

the potential witness discovery materials necessary to prepare them, but may not give or allow the potential witness to retain the discovery materials or copies of them.

5. Each person receiving access to an opposing party's discovery materials other than counsel for the government, law enforcement officers, and counsel for the Defendant, shall first sign and date a copy of this Order to indicate their understanding of, acknowledgment of, and agreement to abide by its terms. Both the Government attorney and Defense counsel shall keep the signed copies in the event of a disclosure or use of discovery materials prohibited by this Order. Neither party shall be required to disclose to the other party who has been given access to what discovery materials, absent further order of this Court following an opportunity to be heard.

6. Defense counsel shall promptly notify the Government and this Court, and Government counsel shall promptly notify Defense counsel and this Court, if any discovery materials are (a) used in a manner inconsistent with this Order or (b) disclosed either intentionally or unintentionally to anyone not designated by this Order or further order of the Court. Each member of the defense and potential witness provided access to discovery materials shall promptly notify defense counsel of any such disclosures.

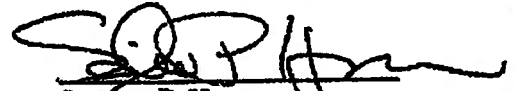
7. At the end of these proceedings, including any potential appeals, the defense shall destroy all copies of discovery materials received and made by it. Defense counsel may keep one copy of all discovery materials for such additional time as they deem necessary to ensure their ability to satisfy all professional obligations to Defendant in this matter. The Government may keep one copy of all defense discovery materials for such additional time as it deems necessary to satisfy its professional obligations and any relevant statutes, regulations, or policies.

8. Nothing in this protective order is intended to otherwise restrict the proper use by the parties of any discovery materials during the investigation, pre-trial litigation, trial preparation, trial or appeal of this matter.

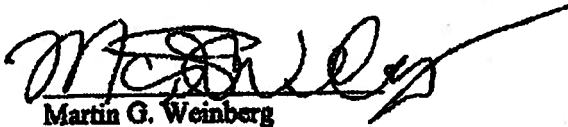
SO STIPULATED.



Aaron Swartz  
Defendant



Stephen P. Heymann  
Scott L. Garland  
Assistant U.S. Attorneys



Martin G. Weinberg  
Defense Counsel

SO ORDERED.



JUDITH G. DEIN  
United States Chief Magistrate Judge

Date: 11/30/11



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES

v.

AARON SWARTZ

No. 11-10260-NMG

**MOTION TO DISMISS COUNTS 1 AND 2 OF INDICTMENT  
AND INCORPORATED MEMORANDUM OF LAW**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court dismiss Counts 1 and 2 of the indictment.

As reason therefor, defendant states:

1. Counts 1 and 2 charge him with wire fraud in violation of 18 U.S.C. §1343.
2. Section 1343 does not encompass the conduct charged in this case.
3. Section 1343 is void for vagueness in violation of the Due Process Clause as applied to the circumstances of this case.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the dismissal remedy sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

Counts 1 and 2 of the indictment charge Swartz with wire fraud in violation of 18 U.S.C. §1343. The indictment alleges that Swartz "having devised and intended to devise a scheme and

RIF

artifice to defraud and for obtaining property – journal articles digitized and distributed by JSTOR, and copies of them – by means of material false and fraudulent pretenses and representations, transmitted and caused to be transmitted by means of wire communication in interstate commerce writings, signs, and signals – that is, communications to and from JSTOR's computer servers – for the purpose of executing the scheme, and aiding and abetting it, including on or about" October 9, 2010, (Count 1) and January 4-6, 2011 (Count 2). Indictment at 10-11, ¶35. Essentially, the indictment alleges that Swartz gained access to the MIT electronic communications network through various mechanisms, and then, having obtained that access, used it to gain access to JSTOR's website, from which he then downloaded a substantial quantity of digitized journal articles.

**I. SECTION 1343 DOES NOT APPLY TO THE CONDUCT CHARGED IN THIS CASE.**

To convict Swartz of an offense under §1343, the government must prove beyond a reasonable doubt: "[his] knowing and willing participation in a scheme or artifice to defraud with the specific intent to defraud, and (2) the use of . . . interstate wire communications in furtherance of the scheme." *United States v. Vazquez-Botet*, 532 F.3d 37, 63 (1st Cir. 2008), quoting *United States v. Sawyer*, 85 F.3d 713, 723 (1st Cir. 1996). An essential element of the offense is that the defendant must have made a *material* misrepresentation or omission of fact. *E.g.*, *Neder v. United States*, 527 U.S. 1, 25 (1999); *Mendez Internet Management Services, Inc. v. Banco Santander de Puerto Rico*, 621 F.3d 10, 15 (1st Cir. 2010); *United States v. Blastos*, 258 F.3d 25, 27 (1st Cir. 2001). A misrepresentation or omission is material only if it has "a natural tendency to influence, or is capable of influencing, the decision of the decisionmaking body to which it is addressed." *United States v. Moran*, 393 F.3d 1, 13 (1st Cir. 2004), quoting *Neder*, 527 U.S. 1, 16. *See, e.g.*, *United*

*States v. Philip Morris USA, Inc.*, 566 F.3d 1095, 1122 (D.C.Cir. 2009)(Materiality requirement is met "if the matter at issue is of importance to a reasonable person making a decision about a particular matter or transaction"); *United States v. Spirk*, 503 F.3d 619, 621 (7th Cir. 2007)(material falsehoods are those "likely to be significant to a reasonable person deciding what to do"); *United States v. Heppner*, 519 F.3d 744, 749 (8th Cir. 2008); *United States v. Lawrence*, 405 F.3d 888, 901 (10th Cir. 2005)("to determine whether a statement is material the appropriate test is to examine whether it has a natural tendency to influence, or is capable of influencing a decision or action by another"). The first fatal flaw in Counts 1 and 2 is that none of the false statements alleged in the indictment were made to a "decisionmaker" or to person making a decision.<sup>1</sup> Instead, they were uniformly statements to a computer or information passed between computers. The indictment alleges the transmission of the following information:

- that when registering as a guest on the MIT network, Swartz used the fictitious names "Gary Host" and "Grace Host," each time obtaining a different IP address; Indictment, ¶14(a), 20, 27(a);
- that when registering as a guest on the MIT network, Swartz gave the computer's client name as "ghost laptop" and "ghost macbook," Indictment, ¶14(b), 20;
- that when registering as a guest on the MIT network, Swartz provided the email address of "ghost@mailinator.com" and "ghost42@mailinator.com," Indictment, ¶14(c), 20;
- that, when JSTOR blocked access to the IP address which Swartz's computer had been using, Swartz established a new IP address which allowed the continued downloading of articles, Indictment, ¶16(b);
- that after MIT blocked access by the computer with the Acer's MAC address, Swartz twice obtained another guest registration by "spoofing," *i.e.*, changing, the Acer's MAC address, again using the name "Gary Host" or "Grace Host" and the client name "ghost laptop," which led to the laptop's receiving a new IP address,

---

<sup>1</sup> Many of them were not in fact material false statements of fact at all. See Section II, *infra*.

Indictment, ¶¶19(a)-(c), 27(a)-(c);

- that during November-December, 2010, Swartz bypassed the guest registration process by connecting directly to the network and assigning himself two new IP addresses, Indictment, ¶24;
- that Swartz, through the use of MIT IP addresses, made it appear that he was affiliated with MIT, Indictment, ¶34(a);
- that Swartz used an automated collection device which made it appear that multiple people were requesting articles rather than a single person making multiple requests, Indictment, ¶34(c).

This information was all either provided by Swartz or Swartz's laptop to MIT's computer network (name, client name, email address) or was information automatically transmitted from one computer to another (IP addresses, MAC addresses, information about the program running). What is wholly missing here is any person or "decisionmaker" to whom the statements – if they were statements at all – were addressed. There was no person or decisionmaker whose "decision" the information had a tendency to influence or was capable of influencing. Nothing in the wire or mail fraud statutes or the case law construing them suggests that their reach extends to information or statements or omissions which are never reviewed or considered by a human being and do not tend to, nor are they capable of, influencing a decision by person. "Materiality" is an element incorporated directly from common law fraud, *see Neder*, 527 U.S. at 21-25, to which the concepts of machines communicating with each other in the complete absence of human agency and of machines robotically performing various functions would have been utterly foreign and incomprehensible, just as the concept that automatic responses by machines constituted "decisionmaking" would have been.

The rule of lenity precludes stretching the wire fraud statute to reach the conduct charged in this case. The rule of lenity "requires ambiguous criminal laws to be interpreted in favor of the

defendants subjected to them.” *United States v. Santos*, 553 U.S. 507, 2025 (2008). See *United States v. Skilling*, 130 S.Ct. 2896, 2932 (2010) (“[A]mbiguity concerning the ambit of criminal statutes should be resolved in favor of lenity”). Critically, the rule of lenity “ensures fair warning by resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered.” *United States v. Lanier*, 520 U.S. 259, 266 (1997).

In various ways over the years, we have stated that when choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite. . . . This principle is founded on two policies that have long been part of our tradition. First, a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so fair as possible the line should be clear. . . . Second, because of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity. This policy embodies the instinctive distastes against men languishing in prison unless the lawmaker has clearly said they should. . . . Thus, where there is ambiguity in a criminal statute, doubts are resolved in favor of the defendant.

*United States v. Bass*, 404 U.S. 336, 347-48 (1971)(internal quotation marks and citations omitted).

Nothing in the wire fraud statute clearly and definitely extends its reach to communications between computers.

In fact, Congress *has* spoken regarding use of computers to commit fraud – but in 18 U.S.C. §1030, not in the wire or mail fraud statutes. Congress’ enactment of §1030(a)(2), criminalizing “intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . [i]nformation from any protected computer” and §1030(a)(4), criminalizing “knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and

obtain[ing] anything of value” – essentially the conduct with which Swartz is charged<sup>2</sup> – provides compelling evidence that it did not believe that such conduct was already encompassed within the reach of the wire fraud statute. Counts 1 and 2 should be dismissed.

**II. THE STATEMENTS AT ISSUE WERE NOT FALSE STATEMENTS OR MISREPRESENTATIONS OR OMISSIONS OF FACT.**

Swartz's giving the computer's client name as “ghost laptop” and “ghost macbook” when registering as a guest on the MIT network,” Indictment, ¶14(b), 20, was not false, and certainly not materially so, because, as the indictment alleges, the client name is one chosen by the user and is simply used to identify the computer on the network. Indictment, ¶14(b). The user is free to choose any name he wishes, and whatever that name is suffices to identify the computer on the network. Here, MIT was always able to identify the computers in use as either “ghost laptop” or “ghost macbook.” The use of those client names was not a fraudulent misrepresentation or omission of material fact.

Similarly, Swartz's providing the email address of “ghost@mailinator.com” and “ghost42@mailinator.com that when registering as a guest on the MIT network,” Indictment, ¶14(c), 20, was also not the making of a false statement. As the indictment acknowledges, the Mailinator email address was a real one through which Swartz could receive email from MIT if its personnel close to communicate with him. The use of those email addresses was not a fraudulent misrepresentation or omission of material fact.

The establishment of a new IP address, Indictment, ¶16(b), is not the making of a false statement. Indeed, it is not a statement at all. “An IP address is an identifier for a computer or device

---

<sup>2</sup> Swartz is charged with violations of these statutes in Counts 3-12.

on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination." [http://www.webopedia.com/TERM/I/IP\\_address.html](http://www.webopedia.com/TERM/I/IP_address.html) (last visited October 2, 2012). Thus, an IP address indicates nothing more than the address the computer is using for communications and is, in fact, always true. Swartz made no false statements or misrepresentations or omissions of material fact when he used different IP addresses to access JSTOR. For the same reasons, Swartz's use of two IP addresses which he allegedly assigned to himself after bypassing the guest registration process and connecting directly to the network, Indictment, ¶24, were not false statements or misrepresentations or omissions of material fact. By the same token, obtaining new IP addresses by "spoofing," i.e., changing, the Acer's MAC address, Indictment, ¶¶19(a)-(c), 27(a)-(c), also cannot constitute false statements or misrepresentations or omissions of material fact, nor can Swartz's use of an automated collection device which made it appear that multiple people were requesting articles rather than a single person making multiple requests, Indictment, ¶34(c).

Swartz's use of MIT IP addresses did not make it appear that he was affiliated with MIT. Indictment, ¶34(a). Instead, MIT had a liberal guest user policy which permitted individuals with no affiliation with MIT whatsoever to access and use the MIT network, *see* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, and Incorporated Memorandum of Law at 9-10; the use of an MIT IP address did not represent to JSTOR that the person seeking access to its website was affiliated with MIT. This, too, did not constitute a material false statement or misrepresentation or omission of fact.

This leaves only Swartz's use of fictitious names when registering on MIT's network as a guest. That statement was made to MIT, not to JSTOR and only allowed Swartz to access the MIT network. It cannot support a charge of devising a scheme to defraud JSTOR of its property, specified

in the indictment as “journal articles digitized and distributed by JSTOR, and copies of them.”

**III. IF §1343 COULD BE APPLIED TO THE CONDUCT CHARGED HERE, IT IS VOID FOR VAGUENESS AS APPLIED TO THIS CASE.**

To pass muster under the Due Process Clause, a statute must give fair warning, “in language that the common world will understand, of what the law intends to do if a certain line is crossed.” *United States v. Hussein*, 351 F.3d 9, 13 (1st Cir. 2003). *See, e.g., United States v. Arcadipane*, 41 F.3d 1, 5 (1st Cir. 1994)(“the Due Process Clause forbids the government from depriving an individual of his liberty unless he is given fair warning of the consequences of that conduct”). “The Due Process Clause demands that criminal statutes describe each particular offense with sufficient definiteness to ‘give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden.’” *Hussein*, 351 F.3d at 13, *quoting United States v. Harriss*, 347 U.S. 612, 617 (1954). *See, e.g., Kolender v. Lawson*, 461 U.S. 352, 357 (1983)(“[A] penal statute [must] define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited” (emphasis added)); *Connally v. General Const. Co.*, 269 U.S. 385, 391 (1926)(“the terms of a penal statute creating a new offense must be sufficiently explicit to inform those who are subject to it what conduct on their part will render them liable to its penalties”(emphasis added)); *United States v. Bohal Trading Co., Inc.*, 45 F.3d 577, 581 (1st Cir. 1995)(issue is “whether the statute, as enacted by Congress, gave sufficient notice that the conduct charged was proscribed” (emphasis added)). In addition, to be valid under the Due Process Clause, penal statutes must be sufficiently specific to prevent arbitrary or discriminatory enforcement. To that end, they must provide comprehensible standards that limit prosecutorial and judicial discretion. *See, e.g., Kolender v. Lawson*, 461 U.S. 352, 357 (1983); *Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972); *Smith v.*



*Goguen*, 415 U.S. 566, 572-73 (1974); *Papachristou v. City of Jacksonville*, 405 U.S. 156, 168 (1972).

As applied to the conduct alleged in this case to have violated §1343, the statute fails to give a person of ordinary intelligence fair notice that conduct such as that charged in this case is forbidden by the statute and could result in criminal prosecution and punishment. Neither the statute, nor any reported judicial decision, “has fairly disclosed” the conduct at issue to be “within [§1343’s] scope.” *Lanier*, 520 U.S. at 266.<sup>3</sup> It may be that the government is seeking to charge a scheme to defraud in

---

<sup>3</sup> This case is not comparable to cases which have applied the wire fraud statute to the distribution and use of devices that enabled users to obtain television or long-distance telephone or internet service without paying for it. See, e.g., *Brandon v. United States*, 382 F.2d 607, 608, 610 (10th Cir.1967)(scheme to defraud telephone company of revenue for the use of long distance telephone service and facilities); *United States v. Manzer*, 69 F.3d 222, 225 (8th Cir.1995)(affirming convictions for wire fraud and mail fraud of a defendant who operated a business whose products enabled users to obtain premium television channels without paying for them); *United States v. Harriss*, 2012 WL 2402788 (D.Mass. June 26, 2012)(upholding against void for vagueness challenge conviction of defendants who sold cable modem hacking products which would permit users to obtain free or higher speed internet access without paying for it); *United States v. Norris*, 833 F.Supp. 1392, 1395-97 (N.D.Ind.1993), *aff’d*, 34 F.3d 530 (7th Cir.1994)(scheme to defraud cable television companies of revenue by selling equipment that allowed individuals to receive premium channels without paying required fee). These cases were held properly prosecuted under the wire fraud statute because the defendants’ products directly enabled their users to defraud the provider of the revenue they would have obtained had the users properly contracted and paid for the services which were instead stolen. Here, in sharp contrast, nothing which Swartz did deprived either MIT or JSTOR of revenue. Guests were entitled to use the MIT network without paying a fee, and, in downloading JSTOR articles, Swartz was not depriving JSTOR of revenue. Moreover, the indictment charges that the property of which JSTOR was defrauded were articles, not revenue.

Nor is this case comparable to *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), in which an IRS employee accessed and viewed confidential material which was the property of his employer. The Court held that the evidence did not suffice to support the defendant’s conviction for wire fraud, but suggested in dictum that the defendant’s conduct might have violated §1343 had he downloaded the confidential material. That dictum is not binding on this Court. See, e.g., *Fletcher v. Haas*, 851 F.Supp.2d 287, 298 (D.Mass. 2012)(quoting Pierre N. Leval, *Judging Under the Constitution: Dicta About Dicta*, 81 N.Y.U. L.Rev. 1249, 1250 (2006)(noting that when judges accept dictum as if it were binding law, they “fail to discharge [their] responsibility to deliberate on and decide the question which needs to be decided”). Moreover, Swartz had no comparable fiduciary duty to JSTOR, the entity from which the articles were downloaded.

the complete absence of material misrepresentations and omissions. However, "the settled meaning of the term 'fraud' at common law required misrepresentation or concealment of a material fact." *United States v. Harriss*, 2012 WL 2402788 at \*4 (D. Mass. June 26, 2012), citing *Neder*, 527 U.S. at 20-25. Nothing in the wire fraud statute or the cases construing it provides constitutionally adequate notice that manipulating IP addresses, spoofing MAC addresses, and gaining access to a free electronic communications network (MIT's) for the purpose of accessing another website to download journal articles which are free to those with access to the website, and for which access MIT had already paid, constitutes a federal wire fraud felony carrying a potential penalty of 30 years. Defendant's research has located no reported wire fraud case which is even remotely comparable to this one. Prosecution of Swartz under §1343 on the theory advanced by the government here would violate Swartz's rights to due process of law. The number of articles downloaded by Swartz may have exceeded JSTOR's terms of service, but the wire fraud statute does not exist to police violations of private contracts. Section 1343 is void for vagueness as applied to this case.

Respectfully submitted,  
By his attorney,

/s/ Martin G. Weinberg  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owimgw@att.net

**CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA.

/s/ Martin G. Weinberg

Martin G. Weinberg

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES

v.

AARON SWARTZ

No. 11-10260-NMG

**MOTION TO SUPPRESS ALL FRUITS OF SEARCHES OF ACER LAPTOP, HP USB  
DRIVE, AND WESTERN DIGITAL HARD DRIVE AND INCORPORATED  
MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 5)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case all evidence derived from the searches of his ACER laptop, his Western Digital hard drive, and his HP USB drive, as well as all derivative fruits thereof.<sup>1</sup>

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his ACER laptop, his Western Digital hard drive, and his HP USB drive.
2. These items were seized without a warrant on January 6, 2011.
3. The Secret Service did not obtain a warrant to search these items until February 9, 2011, Exhibit 38, 34 days after their seizure; that warrant was not executed before its expiration, and another warrant was issued on February 24, 2011, Exhibit 29, 49 days after their seizure.
4. The delay in obtaining search warrants for these items rendered their seizure unreasonable under the Fourth Amendment, requiring that all fruits of the searches of those items be suppressed.

---

<sup>1</sup> All averments herein regarding Swartz's ownership and possession of the ACER laptop, the hard drive, and the USB drive are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

**I. FACTUAL BACKGROUND.**

The ACER laptop and the hard drive were seized without a warrant on January 6, 2011.<sup>2</sup> Shortly thereafter, Swartz was arrested, and the backpack he was carrying was searched and the USB thumb drive seized. S/A Pickett delayed obtaining warrants to search the three items until February 9, 2011, 34 days after their seizure. Even then, he allowed those warrants to expire without executing them. He again applied for warrants to search the three items on February 24, 2011, when warrants authorizing the search of the items were again issued.

**II. SWARTZ HAD A REASONABLE EXPECTATION OF PRIVACY AND A POSSESSORY INTEREST IN HIS ACER LAPTOP, HIS HARD DRIVE, AND HIS USB DRIVE.**

With respect to Swartz's reasonable expectation of privacy and possessory interest in his ACER laptop and his hard drive, Swartz incorporates by reference herein the discussion in Section II of his Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law and in Section II of his Motion to

---

<sup>2</sup> For a recitation of the facts leading up to the seizure of the laptop and hard drive, *see* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, and Incorporated Memorandum of Law, Section I.

Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law. With respect to the USB drive, it belonged to Swartz and was in his backpack when it was searched incident to his arrest and was seized from him at that time. Accordingly, he plainly had a reasonable expectation of privacy in the drive and its contents and a possessory interest in it which its seizure deprived him of.

**III. THE DELAY IN OBTAINING A WARRANT RENDERED THE SEIZURE OF THESE ITEMS UNREASONABLE.**

“[E]ven a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution infringes possessory interests protected by the Fourth Amendment’s prohibition on ‘unreasonable searches.’” *United States v. Jacobson*, 466 U.S. 109, 124 (1984). *See, e.g., Segura v. United States*, 468 U.S. 796, 812 (1984) (“[A] seizure reasonable at its inception because based on probable cause may become unreasonable as a result of its duration”); *United States v. Burgard*, 675 F.3d 1029, 1032 (7th Cir. 2012) (“When officers fail to seek a search warrant, at some point the delay becomes unreasonable and is actionable under the Fourth Amendment”); *United States v. Mitchell*, 565 F.3d 1347, 1350 (11th Cir. 2009) (“even a seizure based on probable cause is unconstitutional if the police act with unreasonable delay in securing a warrant”); *United States v. Riccio*, 2011 WL 4434855 at \*1 (S.D.Cal. Sept. 23, 2011) (“The finding of probable cause to seize the hard drive did not relieve law enforcement of its obligation to ‘diligently’ obtain a warrant,” quoting *United States v. Dass*, 849 F.3d 414, 415 (9th Cir. 1988)).

After seizing an item without a warrant, an officer must make it a priority to secure a search warrant that complies with the Fourth Amendment. This will entail diligent work to present a warrant application to the judicial officer at the earliest reasonable time.



*Burgard*, 675 F.3d at 1035.

In *Mitchell*, the Eleventh Circuit considered a considerably less extensive delay than that present here in obtaining a warrant for the search of a hard drive – 21 days – and held that, under the circumstances of that case, the delay in obtaining a search warrant was unreasonable, thus violating the Fourth Amendment and requiring the suppression of the fruits of the search of the hard drive. In balancing the defendant's possessory interest against the government's interests, the Court first stressed the very strong possessory interests that individuals have in their computers:

Computers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature on their computer hard drives. Thus, the detention of the hard drive for over three weeks before a warrant was sought constitutes a significant interference with Mitchell's possessory interests.

565 F.3d at 1351. Weighed against the defendant's substantial possessory interest, the Court concluded that "there was no compelling justification for the delay." *Id.* Quite the contrary, the Court concluded: law enforcement authorities simply believed that there was "no rush." *Id.* at 1353. The Court made a point of noting that the 23-page affidavit submitted in support of the application for the search warrant was largely boilerplate and contained only three double-spaced pages of original content, *id.* at 1351. *I.e.*, the affidavit would not have taken any substantial amount of time to prepare. Other courts have reached similar conclusions. *See, e.g., United States v. Shaw*, 2012 WL 844075 at \*2-\*4 (N.D.Ga. Feb. 10, 2012)(concluding that 90-day delay in obtaining warrant to search seized cell phones was unreasonable under the Fourth Amendment and recommending that evidence obtained from search of cell phones be suppressed), *adopted*, 2012 WL 843919 (N.D.Ga. March 12, 2012); *Riccio*, 2011 WL 4434855 at \*1 (ordering evidence suppressed where law enforcement delayed 91 days in obtaining a warrant to search defendant's hard drive); *United States*

*v. Rubenstein*, 2010 WL 2723186 at \*13-\*14 (S.D.Fla. June 24, 2010)( recommending suppression of evidence where agents delayed 41 days in obtaining warrant for laptop), *adopted* 2010 WL 2681364 (S.D.Fla. July 7, 2010); *see also United States v. Budd*, 549 F.3d 1140, 1144 (7th Cir. 2008)(assuming without deciding that 48-day delay in obtaining warrant to search computer was unreasonable); *United States v. Kowalczyk*, 2012 WL 3201975 at \*23 (D.Or. Aug. 3, 2012)(terming 7-day delay "unfortunate," but not finding it unreasonable).

Here, there was a 34-day delay in obtaining the February 9, 2011, warrant, which remained unexecuted, and a total of a 49-day delay until the obtaining of the February 24, 2011, warrant pursuant to which the items were ultimately searched. Swartz had a strong possessory interest in all three items. They belonged to him, and he never voluntarily relinquished his dominion and control over them, nor did he ever consent to their seizure. On the other side of the balance, defendant knows of no conceivable reason which could justify a delay of this magnitude. This was a joint investigation involving the Cambridge Police Department, the United States Secret Service and the MIT Police Department, which was being run by S/A Pickett. *See Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, and Incorporated Memorandum of Law, Sections I, IV.* The affidavit submitted in support of the February 9, 2011, warrant application would have taken very little time to prepare. It was only 11 pages in length, plus two attachments describing the property to be seized, the items to be seized, and the objects of the search.<sup>3</sup> *See Exhibit 32.* The first two pages are largely boilerplate, as are pages 9 and 10. Of the remaining content, that

---

<sup>3</sup> In addition to the three items which are the subject of this motion, the application also sought authorization to search Swartz's home. That search is the subject of a separate motion to suppress. *See Motion to Suppress All Fruits of Searches Pursuant to a Warrant of 950 Massachusetts Avenue, Apt. 320, Cambridge, Massachusetts, and 124 Mount Auburn Street, Office 504, Cambridge, Massachusetts and Incorporated Memorandum of Law.*

which applies specifically to this case, it is almost entirely a distillation of previously written reports.<sup>4</sup> *See, e.g., Mitchell*, 565 F.3d at 1351 (indicating Court's belief that 23-page affidavit could have been prepared in the two and a half days before the agent left for two-week training program); *see also Burgard*, 675 F.3d at 1034 (finding it "implausible" that two-page affidavit could not have been prepared in less than six days, particularly as its content was largely derived from previously written reports).

The delay in obtaining the warrants to search the ACER, the hard drive, and the USB drive was unreasonable under the Fourth Amendment. All fruits of the searches of those items must, accordingly, be suppressed.

Respectfully submitted,  
By his attorney,

/s/ Martin G. Weinberg  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net

#### CERTIFICATE OF SERVICE

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to the motion has been served on the government by hand this same date.

/s/ Martin G. Weinberg

Martin G. Weinberg

---

<sup>4</sup> *See, e.g., Exhibit 15.*

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES )

v. )

AARON SWARTZ )

No. 11-10260-NMG

**MOTION TO SUPPRESS ALL FRUITS OF UNLAWFUL ARRESTS WITHOUT  
PROBABLE CAUSE AND SEARCH OF HP USB DRIVE AND INCORPORATED  
MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 3)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case all evidence derived from the search of his HP USB drive.

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his USB drive.<sup>1</sup>
2. The USB drive was seized from him on January 6, 2011, during a search of his backpack incident to his arrest on state charges of breaking and entering in violation of M.G.L. c.266, §18.
3. His arrest was unlawful because not supported by probable cause to believe that he had committed the crime of breaking and entering.
3. On February 9, 2011, Secret Service S/A Michael Pickett obtained a warrant to search the USB drive; that warrant expired before it was executed, and another warrant to search the USB drive was obtained on February 24, 2011. See Exhibit 29. The USB drive was subsequently searched

---

<sup>1</sup> All averments herein regarding Swartz's ownership and possession of the USB drive are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

pursuant to the warrant.

4. The affidavit in support of the search of the USB drive, *see* Exhibit 30, failed to establish probable cause to believe that it contained evidence of a crime, in violation of the Fourth Amendment.

5. All fruits of Swartz's unlawful arrest and the search of the USB drive must, accordingly, be suppressed.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

**I. BACKGROUND.**

On January 6, 2011, Swartz was arrested on state charges of breaking and entering in violation of M.G.L. c.266, §18. *See* Exhibit 31 at 2. The backpack Swartz was carrying was searched and his USB drive, which was in his backpack, was seized. Secret Service S/A Michael Pickett subsequently applied for, and obtained a warrant to search the USB drive. The sum total of the information regarding the USB drive contained in the affidavit submitted in support of the application for a warrant to search the USB drive was:

25. An MIT police officer who had seen several pictures taken by the covert camera in Building 16's network wiring closet saw Aaron Swartz on a bicycle near MIT, approximately half an hour after the "ghost laptop" had been connected in Building W20. The officer stopped his car, activated its blue lights and displayed his wallet badge. When he sought to question Swartz, Swartz dropped his bike to the ground and fled. The backpack

in Swartz's possession at the time he was caught and arrested minutes later appeared to be the same one he had with him on each occasion he was videotaped in the wiring closet at MIT.

26. In the backpack was the USB DRIVE. From my training and experience and information provided to me by other agents, USB drives are frequently used to store software applications, data and records, including .pdf formatted records such as those that were illegally downloaded from JSTOR. They are also frequently used to transfer records and data between computers or hard drives, such as those connected in the wiring closet to MIT's network and ones available to Swartz outside.

Exhibit 30 at 7.<sup>2</sup>

**II. SWARTZ'S ARREST WAS UNLAWFUL BECAUSE NOT SUPPORTED BY PROBABLE CAUSE TO BELIEVE THAT HE COMMITTED THE MASSACHUSETTS OFFENSE OF BREAKING AND ENTERING.**

It is axiomatic that, for an arrest to be lawful, it must be predicated on probable cause. See *Gilk v. Cunniffe*, 655 F.3d 78, 85 (1st Cir. 2011) ("The Fourth Amendment requires that an arrest be grounded in probable cause"). "Probable cause exists when police officers, relying on reasonably trustworthy facts and circumstances, have information upon which a reasonably prudent person would believe the suspect had committed or was committing a crime." *United States v. Pontoo*, 666 F.3d 20, 31 (1st Cir. 2011), quoting *United States v. Young*, 105 F.3d 1, 6 (1st Cir. 1997). That standard was not satisfied in this case.

Swartz was arrested on charges of breaking and entering in violation of M.G.L. c.266, §18, which provides:

Whoever, in the night time, enters a dwelling house without breaking, or breaks and enters in the day time a building, ship or motor vehicle or vessel, with intent to commit a felony, no person lawfully therein being put in fear, shall be punished by imprisonment in the state

---

<sup>2</sup> Other than the fact that the USB drive was in the backpack, the information set forth in paragraph 26 was not included in the original February 9, 2011, affidavit, *i.e.*, the affidavit said nothing regarding what a USB drive is and what it might be used for. That affidavit also erroneously stated that Swartz "dropped his bike *and backpack* to the ground and fled," Exhibit 32 at 7 (emphasis added), as S/A Pickett admits at page 7 n.5 of his February 24, 2011, affidavit.



prison for not more than ten years or by a fine of not more than five hundred dollars and imprisonment in jail for not more than two years. . . .

The first requirement under §18 is that there must have been a "breaking." While the opening of a closed but unlocked door is a breaking, passing through an unobstructed entrance is not. *Commonwealth v. Lewis*, 346 Mass. 373, 377 (1963). Thus, to have probable cause to arrest Swartz, the arresting officers must have had probable cause to believe that he in fact opened a door to enter the data room in which the laptop was discovered. Moreover, MIT is an open campus, and the data room was located on a corridor along which classrooms were located and along which people frequently passed to access classrooms or to travel between MIT buildings. There was no notice on the exterior of the data room indicating that access was prohibited. *See Exhibit 27*. Inherent in the offense of breaking and entering is the requirement that the defendant break and enter into premises where he has no permission to be, a proposition that Massachusetts case law clearly supports. *See, e.g., Commonwealth v. LeClaire*, 28 Mass. App. Ct. 932, 933 (1990)(upholding breaking and entering conviction where defendant broke into room *where he had no permission or authority to be*). There was nothing here which gave Swartz any reason to believe that he could not permissibly enter the room.

Second, "[i]n the lexicon of Massachusetts crimes there is no such crime as 'breaking and entering' unaccompanied by intent to commit a felony or misdemeanor." *Commonwealth v. Vinnicombe*, 28 Mass. App. Ct. 934, 934 (1990). *See, e.g., Commonwealth v. Walter*, 40 Mass. App. Ct. 907, 909 (1996)("The 'intent to commit a felony' is an essential element of the crime proscribed by G.L. c.266, §18, breaking and entering in the daytime with intent to commit a felony"). Accordingly, there could have been no probable cause to arrest Swartz unless the arresting officers

had probable cause to believe that his intent in entering the data room was to commit a felony. The Cambridge Police Department Incident Report of the arrest does not specify the felony at issue, but, as Swartz was charged in state court with breaking and entering with the intent to commit larceny on January 4 and 6, 2011, Swartz will proceed herein on the assumption that that was the offense which the arresting officers believed provided a valid basis for his arrest. It did not. The Massachusetts larceny statute, M.G.L. c.266, §30, provides in pertinent part:

(1) Whoever steals, or with intent to defraud obtains by a false pretence, or whoever unlawfully, and with intent to steal or embezzle, converts, or secretes with intent to convert, the property of another as defined in this section, whether such property is or is not in his possession at the time of such conversion or secreting, shall be guilty of larceny, and shall . . . if the value of the property stolen exceeds two hundred and fifty dollars, be punished by imprisonment in the state prison for not more than five years, or by a fine of not more than twenty-five thousand dollars and imprisonment in jail for not more than two years; or, if the value of the property stolen . . . does not exceed two hundred and fifty dollars, shall be punished by imprisonment in jail for not more than one year or by a fine of not more than three hundred dollars . . . .

(2) The term "property", as used in the section, shall include money, personal chattels, a bank note, bond, promissory note, bill of exchange or other bill, order or certificate, a book of accounts for or concerning money or goods due or to become due or to be delivered, a deed or writing containing a conveyance of land, any valuable contract in force, a receipt, release or defeasance, a writ, process, certificate of title or duplicate certificate issued under chapter one hundred and eighty-five, a public record, anything which is of the realty or is annexed thereto, a security deposit received pursuant to section fifteen B of chapter one hundred and eighty-six, electronically processed or stored data, either tangible or intangible, data while in transit, telecommunications services, and any domesticated animal, including dogs, or a beast or bird which is ordinarily kept in confinement.

Thus, to have had probable cause to believe that Swartz entered the data room with the intent to commit larceny, the arresting officers must have had probable cause to believe that he either intended to steal property or to obtain property by false pretenses with the intent to defraud.<sup>3</sup> An essential

---

<sup>3</sup> The third alternative, embezzlement, is inapplicable here because embezzlement requires that the defendant "fraudulently converted to his personal use property that was under his control by

element of the "stealing" form of larceny is the "intent to deprive the person of the property permanently." *Commonwealth v. Christian*, 430 Mass. 552, 558 (2000). See, e.g., *Commonwealth v. Sullivan*, 40 Mass. App. Ct. 284, 287 (1996) ("Larceny consists of (1) the taking or carrying away of property (2) that belongs to another person (3) with the intent to deprive that person of the property permanently"). Nothing which Swartz did in downloading journal articles from JSTOR was intended to deprive JSTOR of its property permanently, nor did the downloading even have that effect. JSTOR remained at all times in full possession of its property, and nothing Swartz did on January 4-6, 2011, prevented others from gaining access to, and using, the JSTOR archives. There is nothing in Massachusetts law which recognizes the electronic copying of data as larceny.<sup>4</sup> Accordingly, there was no probable cause to arrest Swartz for breaking and entering to commit larceny by stealing.

Nor was there probable cause to arrest Swartz for larceny by false pretenses. The crime of

---

virtue of a position of 'trust or confidence' and did so with the intent to deprive the owner of the property permanently." *Commonwealth v. Mills*, 436 Mass. 387, 394 (2002).

<sup>4</sup> That copying of electronically-available data is not encompassed within §30(1) is underscored by the provisions of §30(4):

Whoever steals, or with intent to defraud obtains by a false pretense, or whoever unlawfully, and with intent to steal or embezzle, converts, secretes, unlawfully takes, carries away, conceals or copies with intent to convert any trade secret of another, regardless of value, whether such trade secret is or is not in his possession at the time of such conversion or secreting, shall be guilty of larceny . . . .

(emphasis added). The inclusion of copying in subsection (4) but not in subsection (1) evidences an intent that copying does not violate subsection (1), as it does not permanently deprive the owner of its property. Copying violates the statute only in cases of trade secrets, which are not at issue here. See §30(4)(defining "trade secrets" as "anything tangible or intangible or electronically kept or stored, which constitutes, represents, evidences or records a secret scientific, technical, merchandising, production or management information, design, process, procedure, formula, invention or improvement").

larceny by false pretenses "requires proof that (1) a false statement of fact was made; (2) the defendant knew or believed that the statement was false when he made it; (3) the defendant intended that the person to whom he made the false statement would rely on it; and (4) the person to whom the false statement was made did rely on it and, consequently, parted with property." *Commonwealth v. McCauliff*, 461 Mass. 635, 639-39 (2012). See, e.g., *Commonwealth v. Mills*, 436 Mass. 387, 396-97 (2002); *Commonwealth v. Gall*, 58 Mass. App. Ct. 278, 285 (2003). First, Swartz made no false statements of fact on January 4-6, 2011. Second, even if he had made a false statement, it was not made to JSTOR, nor was it made with the intent that JSTOR would rely on it, JSTOR did not rely on any false statement by Swartz, and no false statements by Swartz caused JSTOR to part with its property. Third, JSTOR did not "part with" its property. It simply permitted Swartz to access it and download it; JSTOR continued to maintain full possession of its property. There was, accordingly, no probable cause to arrest Swartz for breaking and entering to commit larceny by false pretenses. Because Swartz's arrest was unlawful, all fruits of that unlawful arrest, including, but not limited to, his USB drive, must be suppressed.

**III. EVEN SHOULD THIS COURT CONCLUDE THAT SWARTZ'S ARREST WAS LAWFUL, THE FRUITS OF THE SEARCH OF THE USB DRIVE MUST NONETHELESS BE SUPPRESSED BECAUSE THE AFFIDAVIT FAILED TO ESTABLISH PROBABLE CAUSE FOR THE SEARCH OF THE USB DRIVE.**

Probable cause exists when "the affidavit upon which a warrant is founded demonstrates in some trustworthy fashion the likelihood that an offense has been committed and that there is sound reason to believe that a particular search will turn up evidence of it." *United States v. Schaefer*, 87 F.3d 562, 565 (1st Cir. 1996), quoting *United States v. Aguirre*, 839 F.2d 854, 857-58 (1st Cir. 1988). "[M]ere suspicion, rumor, or strong reason to suspect [wrongdoing]' are not sufficient."

*United States v. Vigeant*, 176 F.3d 565, 569 (1st Cir. 1999). Instead, the affidavit must provide the issuing judge with a “substantial basis” for concluding that probable cause exists. See, e.g., *United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999); *United States v. Khounsavanh*, 113 F.3d 279, 283 (1st Cir.1997).

While courts often speak of the need to accord deference to the issuing judge’s “assessment of the facts and inferences supporting the affidavit,” *United States v. Sawyer*, 144 F.3d 191, 193 (1st Cir. 1998), “[d]eference to the [issuing] magistrate . . . is not boundless.” *United States v. Leon*, 468 U.S. 897, 914 (1984). See, e.g., *United States v. Danhauer*, 229 F.3d 1002, 1006 (10th Cir. 2000)(court will not defer to magistrate if there is not substantial basis for concluding that probable cause existed). Such deference does not, for example, extend to permit the upholding of a warrant based on conclusory allegations by the affiant. See, e.g., *Vigeant*, 176 F.3d at 571; *United States v. Wilhelm*, 80 F.3d 116, 119 (4th Cir.1996). “Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others.” *Illinois v. Gates*, 462 U.S. 213, 239 (1983). See also *Johnson v. United States*, 333 U.S. 10, 14 (1947); *Khounsavanh*, 113 F.3d at 284. Probable cause is a fact-specific inquiry, and it is, in each case, “the duty of a court confronted with the question to determine whether the facts and circumstances of the particular [affidavit in support of a warrant application] justified the issuance of the warrant.” *Id.* at 285. See also *United States v. Weaver*, 99 F.3d 1372, 1376-77 (6th Cir.1996).

“A warrant application must demonstrate probable cause to believe that (1) a crime has been committed – the ‘commission’ element, and (2) enumerated evidence of the offense will be found at the place to be searched – the . . . ‘nexus’ element.” *United States v. Ribeiro*, 397 F.3d 43, 48 (1st

Cir. 2005), *quoting Feliz*, 182 F.3d at 86. S/A Pickett's affidavit is fatally deficient as to the second requirement – it fails to establish probable cause to believe that evidence of the alleged crime would be found on the USB drive. Whether there is probable cause to believe that the suspect has committed a crime and whether there is a nexus between evidence of that crime and the place or item to be searched are two separate inquiries; probable cause to believe that someone has committed a crime does not *ipso facto* provide probable cause to believe that evidence of that crime will be found within a closed container belonging to him. “The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific ‘things’ to be searched for and seized are located on the property to which entry is sought.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978). There must be “some type of evidence connecting the criminal activity, not just the suspect, to the place to be searched.” *United States v. Kemper*, 375 F.Supp.2d 551, 553 (E.D.Ky. 2005). *See, e.g., United States v. Rosario*, 918 F.Supp. 524, 531 (D.R.I. 1996); *United States v. Rios*, 881 F.Supp. 772, 775 (D.Conn. 1995); *United States v. Stout*, 641 F.Supp. 1074, 1078 (N.D.Cal. 1986). Any contrary rule “would be an open invitation to vague warrants authorizing virtually automatic searches of any property used by a criminal suspect.” *Rosario*, 918 F.Supp. at 531. *See also United States v. Schultz*, 14 F.3d 1093, 1098 (6th Cir. 1994); *Rios*, 881 F.Supp. at 775; *Stout*, 641 F.Supp. at 1078.

Here, the requisite nexus is absent. Swartz may have been carrying the USB drive in his backpack, and that backpack may have accompanied him when he visited the basement data room at MIT, but what is entirely missing is any connection between the USB drive and the alleged offense. The possession of a USB drive connotes nothing nefarious. Quite the contrary, USB drives – often referred to as thumb drives or flash drives or memory sticks – are common accoutrements



of modern life, used by millions of people every day for storing and transporting a wide variety of personal and professional documents, as well as other information, and, for example, photographs, videos, audio files, and games. See [http://en.wikipedia.org/wiki/USB\\_flash\\_drive](http://en.wikipedia.org/wiki/USB_flash_drive). The videotape never showed Swartz using the USB drive in connection with the JSTOR downloads. Quite the contrary, in fact. The videotape showed a far larger external hard drive attached to the ACER laptop which was connected to the MIT network and showed Swartz retrieving one hard drive and exchanging it for another, *i.e.*, it showed that, to the extent that Swartz was using any portable medium to store and transport downloaded JSTOR data, it was not a USB drive but instead an external hard drive. Neither the laptop nor the hard drive was in Swartz's backpack when it was seized but were instead seized later from a separate location at MIT.

While S/A Pickett did add some experiential generalities about what USB drives can be used for, there is nothing in the affidavit which factually connects those potential uses to the circumstances of this particular case. Such generalities are entitled to little or no weight, as the affidavit did not provide a sufficient factual basis for the Magistrate Judge to make a neutral, independent determination that the generalities recited by S/A Pickett were likely to be true with respect to the particular search for which authorization was being sought. See, *e.g.*, *Ribeiro*, 397 F.3d at 52 (generalizations alone may not be enough to satisfy the nexus element); *Zimmerman*, 277 F.3d 416, 433 n.3 (3d Cir. 2002) (expert opinion "must be tailored to the specific facts of the case to have any value"); *Schultz*, 14 F.3d at 1097 (officer's training and experience "cannot substitute for the lack of evidentiary nexus"). The affidavit failed to establish probable cause for the search of the USB drive.

**IV. THE GOOD FAITH EXCEPTION CANNOT SAVE THE SEARCH OF THE USB DRIVE, AND ALL FRUITS OF THAT SEARCH MUST BE SUPPRESSED.**

The government has the burden to demonstrate the applicability of the good faith exception, *see, e.g., United States v. Diehl*, 276 F.3d 32, 42 (1st Cir. 2002), and unless it can meet that burden, the evidence must be suppressed. It will not be able to do so in this case. “Although weakening the exclusionary rule, the [*Leon*] Court did not defenestrate it.” *United States v. Ricciardelli*, 998 F.2d 8, 15 (1st Cir. 1993). “Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble.” *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996), *aff’d on rehearing*, 91 F.3d 331 (1996). The determination whether the *Leon* good faith exception should be applied in a particular case requires an “inquir[y] into the ‘objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate’s authorization.’” *United States v. Diaz*, 841 F.2d 1, 5 (1st Cir. 1998), *quoting United States v. Leon*, 468 U.S. 897, 922 n.23 (1984).

The good faith exception does not apply when the affidavit was “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.” *Leon*, 468 U.S. at 922. Where the defect in the warrant is one of probable cause, the requisite inquiry is “whether a reasonably well-trained officer . . . would have known that his affidavit failed to establish probable cause and that he should not have applied for the warrant.” *Vigeant*, 176 F.3d at 571, *quoting Malley v. Briggs*, 475 U.S. 335, 345 (1985). Here, a reasonably well-trained officer would have known that the affidavit failed to establish probable cause as to the essential “nexus” element of probable cause. *See, e.g., United States v. Grant*, 682 F.3d 827, 841 (9th Cir. 2012); *United States v. Laughton*, 409 F.3d 744, 749 (6th Cir. 2005); *Zimmerman*, 277 F.3d at 437-38; *Kemper*, 375 F.Supp.2d at 554-55.

The Court should, therefore, find the good faith exception inapplicable.

**CONCLUSION**

For all the foregoing reasons, all fruits of Swartz's unlawful arrest and the search of the USB drive must be suppressed as evidence at the trial of this case.

Respectfully submitted,

By his attorney,

/s/ Martin G. Weinberg

Martin G. Weinberg

20 Park Plaza, Suite 1000

Boston, MA 02116

(617) 227-3700 (tel.)

(617) 338-9538 (fax)

owlmgw@att.net

**CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to the motion was served on the government by hand this same date.

/s/ Martin G. Weinberg

Martin G. Weinberg

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES

v.

AARON SWARTZ

No. 11-10260-NMG

**MOTION TO SUPPRESS ALL FRUITS OF SEARCHES PURSUANT TO A WARRANT  
OF 950 MASSACHUSETTS AVENUE, APT. 320, CAMBRIDGE, MASSACHUSETTS,  
AND 124 MOUNT AUBURN STREET, OFFICE 504, CAMBRIDGE, MASSACHUSETTS  
AND INCORPORATED MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 4)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case all evidence derived from searches of his home at 950 Massachusetts Avenue, Apt. 320, Cambridge, Massachusetts, and of his office at 124 Mount Auburn Street, Office 504, Cambridge, Massachusetts.

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his home and in his office.
2. On February 9, 2011, Secret Service S/A Michael Pickett submitted an affidavit in support of an application for a warrant to search Swartz's home at 950 Massachusetts Avenue, Apt. 320, Cambridge, Massachusetts. Exhibit 34. A warrant authorizing the search was issued the same day. Exhibit 35. The search warrant was executed on February 11, 2011.
3. The affidavit submitted in support of the warrant application failed to establish probable cause to believe that evidence of the alleged offense would be found in Swartz's home, in violation of the Fourth Amendment.
4. On February 11, 2011, Secret Service S/A Brett Seidel submitted an affidavit in support

of an application for a warrant to search Swartz's office at 124 Mount Auburn Street, Office 504, Cambridge, Massachusetts, the case-specific averments of which were virtually entirely derived from observations made by law enforcement officers during the search of Swartz's home and statements made by Swartz which were a direct product of that search. Exhibit 36. The warrant was issued and executed the same day. Exhibit 37.

5. The warrant to search Swartz's office was devoid of probable cause to believe that the items sought would be located there. The probable cause averments of the affidavit were derived from the unlawful search of his home; with those portions of the affidavit excised, as they must be, the affidavit failed to establish probable cause for the search. Alternatively, even if the earlier search of his home were found not to have violated the Fourth Amendment, the affidavit did not establish probable cause to search Swartz's office.

6. All fruits of both searches must, accordingly, be suppressed.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

**I. THE SEARCH OF SWARTZ'S HOME.**

**A. Swartz Had A Reasonable Expectation of Privacy in his Home.**

"An individual's right to be free from unreasonable searches is implicated when he or she (1) has "manifested a subjective expectation of privacy" in the place searched, which (2) "society

accepts as objectively reasonable." *United States v. Cardona-Sandoval*, 6 F.3d 15, 20 (1st Cir. 1993), quoting *California v. Greenwood*, 486 U.S. 35, 39 (1988). See, e.g., *United States v. Mancini*, 8 F.3d 104, 107 (1st Cir. 1993). The apartment at 950 Massachusetts Avenue, Apt. 320, Cambridge, Massachusetts, was Swartz's home at the time of the search. He had a subjective expectation of privacy in his home, and that expectation is one which society would certainly accept as objectively reasonable.

**B. The Averments of the Affidavit.**

After reciting information based on which S/A Pickett believed that a crime had been committed and that Swartz had committed it, none of which was in any way related to Swartz's home, Exhibit 34 at 3-7, the affidavit had only this to say about Swartz's home:

26. It is probable that Aaron Swartz stores and uses computer equipment, computer hardware, computer software, computer related documentation, data and records, as defined in Attachment B, at 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts, where he lives.

\* \* \* \* \*

30. Swartz has provided 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts to the Commonwealth as his home address. It is also the address of record for Demand Progress, Inc., of which he is the registered agent, director, president and treasurer. Demand Progress maintains a website, in which it describes its mission in part to seek progressive policy changes by running online campaigns.

Exhibit 34 at 7 -8.<sup>1</sup> The affidavit also mentioned that neither the "ghost macbook" associated with the JSTOR downloading or the external hard drive which had been observed attached to the ACER laptop on January 4, 2011, had yet been recovered. *Id.* The affidavit further stated that on January 10, 2011, Swartz "broadcast a message via Twitter for Mac." *Id.* Finally, S/A Pickett included a boilerplate recitation of the purposes for which individuals in general use computers, noting that 86%

---

<sup>1</sup> Paragraph 31 of the affidavit goes on to provide a description of the premises.



of all households owned at least one computer. *Id.* at 8.

**C. The Affidavit Failed to Establish Probable Cause to Believe That the Items Sought Would Be Located At Swartz's Home at the Time of the Search.**

Probable cause exists when "the affidavit upon which a warrant is founded demonstrates in some trustworthy fashion the likelihood that an offense has been committed and that there is sound reason to believe that a particular search will turn up evidence of it." *United States v. Schaefer*, 87 F.3d 562, 565 (1st Cir. 1996), quoting *United States v. Aguirre*, 839 F.2d 854, 857-58 (1st Cir. 1988). "[M]ere suspicion, rumor, or strong reason to suspect [wrongdoing]' are not sufficient." *United States v. Vigeant*, 176 F.3d 565, 569 (1st Cir. 1999). Instead, the affidavit must provide the issuing judge with a "substantial basis" for concluding that probable cause exists. See, e.g., *United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999); *United States v. Khounsavanh*, 113 F.3d 279, 283 (1st Cir.1997).

While courts often speak of the need to accord deference to the issuing judge's "assessment of the facts and inferences supporting the affidavit," *United States v. Sawyer*, 144 F.3d 191, 193 (1st Cir. 1998), "[d]eference to the [issuing] magistrate . . . is not boundless." *United States v. Leon*, 468 U.S. 897, 914 (1984). See, e.g., *United States v. Danhauer*, 229 F.3d 1002, 1006 (10th Cir. 2000)(court will not defer to magistrate if there is not substantial basis for concluding that probable cause existed). Such deference does not, for example, extend to permit the upholding of a warrant based on conclusory allegations by the affiant. See, e.g., *Vigeant*, 176 F.3d at 571; *United States v. Wilhelm*, 80 F.3d 116, 119 (4th Cir.1996). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *Illinois v. Gates*, 462 U.S. 213, 239 (1983). See also *Johnson*

*v. United States*, 333 U.S. 10, 14 (1947); *Khounsavanh*, 113 F.3d at 284. Probable cause is a fact-specific inquiry, and it is, in each case, “the duty of a court confronted with the question to determine whether the facts and circumstances of the particular [affidavit in support of a warrant application] justified the issuance of the warrant.” *Id.* at 285. *See also United States v. Weaver*, 99 F.3d 1372, 1376-77 (6th Cir.1996).

“A warrant application must demonstrate probable cause to believe that (1) a crime has been committed – the ‘commission’ element, and (2) enumerated evidence of the offense will be found at the place to be searched – the . . . ‘nexus’ element.” *United States v. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005), *quoting United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999). In deciding whether the affidavit demonstrates such the requisite nexus between the items sought and the place to be searched, the judicial officer must determine “whether the totality of circumstances reasonably inferable from the affidavit demonstrates a ‘fair probability’ that evidence material to the ‘commission’ of the probable crime will be disclosed at the search premises at about the time the search warrant would issue . . .” *United States v. Zayas-Diaz*, 95 F.3d 105, 113 (1st Cir. 1996). *See, e.g., Ribeiro*, 397 F.3d at 48-49; *Feliz*, 182 F.3d at 86. Nexus need not rest on any direct observation, but may be inferred from the type of crime, the nature of the items sought, the extent of an opportunity for concealment and normal inferences as to where a criminal would hide [evidence of the crime].” *Feliz*, 182 F.3d at 88.

Whether there is probable cause to believe that the suspect has committed a crime and whether there is a nexus between evidence of that crime and the place to be searched are two separate inquiries; probable cause to believe that someone has committed a crime does not *ipso facto* provide probable cause to believe that evidence of that crime will be found in his home or office.

"The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978). There must be "some type of evidence connecting the criminal activity, not just the suspect, to the place to be searched." *United States v. Kemper*, 375 F.Supp.2d 551, 553 (E.D.Ky. 2005). See, e.g., *United States v. Rosario*, 918 F.Supp. 524, 531 (D.R.I. 1996); *United States v. Rios*, 881 F.Supp. 772, 775 (D.Conn. 1995); *United States v. Stout*, 641 F.Supp. 1074, 1078 (N.D.Cal. 1986). Any contrary rule "would be an open invitation to vague warrants authorizing virtually automatic searches of any property used by a criminal suspect." *Rosario*, 918 F.Supp. at 531. See also *United States v. Schultz*, 14 F.3d 1093, 1098 (6th Cir. 1994); *Rios*, 881 F.Supp. at 775; *Stout*, 641 F.Supp. at 1078.

S/A Pickett's affidavit completely failed to demonstrate probable cause to believe that the items sought would be found in Swartz's home at the time of the search. The warrant was applied for, and issued, more than a month after Swartz was arrested on January 6, 2011. The alleged offenses at issue were not shown to have had any connection to Swartz's home. The laptops through which the JSTOR downloads were conducted were located on MIT premises and used the MIT network to access JSTOR. Swartz was not observed going from his apartment to MIT or going directly from accessing the laptop and hard drive at MIT to his apartment. Nothing in the affidavit even inferentially connects the items sought with Swartz's apartment. Compare, e.g., *United States v. Laughton*, 409 F.3d 744, 474 (6th Cir. 2005) (ordering evidence suppressed where affidavit failed to make any connection between the residence to be searched and the facts of the criminal activity set forth in the affidavit); *Kemper*, 375 F.Supp.2d at 554 (ordering evidence suppressed where no

nexus shown between residence and the criminal activity as to which evidence sought), *with, e.g., Ribeiro*, 397 F.3d at 52 (affidavit set forth police observations of defendant leaving residence in close temporal proximity to drug transactions); *United States v. Keene*, 341 F.3d 78, 82 (1st Cir. 2003)(fact that defendant worked from home while recovering from injury suggested that drug distribution was being organized from defendant's home). Even if one indulged in the unwarranted assumption that the twitter message referenced by S/A Pickett was sent from the same macbook used during the JSTOR downloads, the macbook, being readily portable, could have been located anywhere when the message was sent; this information provides no nexus between the macbook and Swartz's apartment. On the critical nexus component of the probable cause calculus, the affidavit provided the Magistrate Judge with little more than S/A Pickett's bare-bones claim that "[i]t is probable" that the items sought would be found at Swartz's home.<sup>2</sup> Such conclusory allegations by the affiant, not even accompanied by standard boilerplate regarding what the affiant's training and experience tell him about where individuals maintain evidence of crimes, does not suffice to establish probable cause.

**D. The Good Faith Exception Cannot Save the Search of Swartz's Home, and All Fruits of That Search must Be Suppressed.**

The government has the burden to demonstrate the applicability of the good faith exception,

---

<sup>2</sup> While S/A Pickett did add some experiential generalities about what computers can be used for, there is nothing in the affidavit which factually connects those potential uses to the circumstances of this particular case. Such generalities are entitled to little or no weight, as the affidavit did not provide a sufficient factual basis for the Magistrate Judge to make a neutral, independent determination that the generalities recited by S/A Pickett were likely to be true with respect to the particular search for which authorization was being sought. *See, e.g., Ribeiro*, 397 F.3d at 52 (generalizations alone may not be enough to satisfy the nexus element); *Zimmerman*, 277 F.3d 416, 433 n.3 (3d Cir. 2002)(expert opinion "must be tailored to the specific facts of the case to have any value"); *Schultz*, 14 F.3d at 1097 (officer's training and experience "cannot substitute for the lack of evidentiary nexus").

*see, e.g., United States v. Diehl*, 276 F.3d 32, 42 (1st Cir. 2002), and unless it can meet that burden, the evidence must be suppressed. It will not be able to do so in this case. “Although weakening the exclusionary rule, the [*Leon*] Court did not defenestrate it.” *United States v. Ricciardelli*, 998 F.2d 8, 15 (1st Cir. 1993). “Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble.” *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996), *aff’d on rehearing*, 91 F.3d 331 (1996). The determination whether the *Leon* good faith exception should be applied in a particular case requires an “inquir[y] into the ‘objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate’s authorization.’” *United States v. Diaz*, 841 F.2d 1, 5 (1st Cir. 1998), *quoting United States v. Leon*, 468 U.S. 897, 922 n.23 (1984).

The good faith exception does not apply when the affidavit was “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.” *Leon*, 468 U.S. at 922. Where the defect in the warrant is one of probable cause, the requisite inquiry is “whether a reasonably well-trained officer . . . would have known that his affidavit failed to establish probable cause and that he should not have applied for the warrant.” *Vigeant*, 176 F.3d at 571, *quoting Malley v. Briggs*, 475 U.S. 335, 345 (1985). Here, a reasonably well-trained officer would have known that the affidavit failed to establish probable cause as to the essential “nexus” element of probable cause. *See, e.g., United States v. Grant*, 682 F.3d 827, 841 (9th Cir. 2012); *United States v. Laughton*, 409 F.3d 744, 749 (6th Cir. 2005); *Zimmerman*, 277 F.3d at 437-38; *Kemper*, 375 F.Supp.2d at 554-55. The Court should, therefore, find the good faith exception inapplicable. Accordingly, all fruits of the search of Swartz’s home, including, but not limited to, statements made by him to law enforcement officers during the search.

## **II. THE SEARCH OF SWARTZ'S OFFICE.**

### **A. Swartz Had a Reasonable Expectation of Privacy in his Office.**

The office which was searched was Swartz's private office at the Safra Center for Ethics at Harvard, where he was a fellow. He did not share it with others, and the door had a lock on it. The computer in the office was password-protected. He had a both a subjective and an objectively reasonable expectation of privacy in his office. *See, e.g., United States v. Ziegler*, 474 F.3d 1184, 1189-90 (9th Cir. 2007); *O'Rourke v. Hayes*, 378 F.3d 1201, 1208 (11th Cir. 2004); *United States v. Mancini*, 8 F.3d 104, 109-10 (1st Cir. 1993).

### **B. The Search of Swartz's Office Was the Derivative Fruit of the Unlawful Search of Swartz's Home.**

The probable cause averments of the affidavit are virtually entirely derived from observations made by law enforcement officers at the time of the search of Swartz's home and statements made by Swartz during, and as the direct product of, the search – that during the search, law enforcement officers observed computer wiring and computer paraphernalia, but no computers, that Swartz said during the search, “what took you so long” and “Why didn't you do this earlier?”, that Swartz left the building when the agents did and began running, and that Swartz was thereafter located at his office at 124 Mount Auburn Street, Suite 520N. Exhibit 36, ¶¶6-9.<sup>3</sup> Indeed, the affidavit's nexus recitations rely virtually exclusively on the fruits of the unlawful search of Swartz's home: “Based on Swartz's statements during the search, the fact that computer hardware had clearly been removed from his apartment, his conduct immediately after the search, the remote access capabilities of the

---

<sup>3</sup> In ¶11, the affidavit discusses the results of the port scan of Swartz's laptop, which was itself an unlawful search. *See* Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011, to January 6, 2011, And Incorporated Memorandum of Law.

Acer laptop installed at MIT in furtherance of the crimes, and on my training and experience, I believe that it is probable that Swartz ran from the apartment after the search to locate, hide and/or destroy evidence, fruits, or instrumentalities at his office." Exhibit 36, ¶14. Absent the information gleaned as the direct result of the unlawful search of Swartz's home, the affidavit does not establish probable cause to believe that evidence of the alleged offense would be found in Swartz's office. All evidence seized pursuant to this warrant, as well as all derivative fruits thereof, must be suppressed.

**C. Even if the Information Which Was the Product of the Search of Swartz's Home is Considered, the Affidavit Failed to Establish Probable Cause to Search Swartz's Office.**

The information set forth in the affidavit fails to provide probable cause to believe that evidence of the alleged offenses would be found in Swartz's office. See pages 4-6, *supra*. Swartz's statements to law enforcement officers during the search of his home, on which the affiant relies, Exhibit 36, ¶¶6, 14, provide no basis for an inference that evidence of the alleged crime was located at Swartz's office, nor do the remote capabilities of the Acer laptop, Exhibit 36, ¶¶11, 14, which had long since been seized by law enforcement. That Swartz had "computer hardware" in his office, Exhibit 36, ¶13, does not establish a connection with the alleged offenses. It is a rare office indeed in these days that does not contain computer hardware. The only computer hardware associated with the alleged offenses was the Acer laptop and the hard drive seized on January 4, 2011, and a macbook and a Samsung hard drive, and the affidavit provides no reason to believe that either of the latter two would be found in Swartz's office. The only connection shown with Swartz's office is that he was observed to run there after his home was searched. That observation does not provide probable cause to believe that evidence of the alleged offenses would be found in Swartz's office; indeed, that Swartz went to his office immediately following the search of his home, going past the



officers who searched his home to do so and with them observing him, would suggest quite the opposite of his going to his office for the purpose of destroying or removing evidence.

**D. The Good Faith Exception Cannot Save the Search of Swartz's Office, and All Fruits of That Search must Be Suppressed.**

The good faith exception cannot save the unlawful search of Swartz's office for the same reasons addressed in Section I(D), *supra*.

Respectfully submitted,  
By his attorney,

/s/ Martin G. Weinberg  
Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
ow/mgw@att.net

**CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to this motion was served on the government by hand this same date.

/s/ Martin G. Weinberg

Martin G. Weinberg



UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES

v.

AARON SWARTZ

No. 11-10260-NMG

**MOTION TO SUPPRESS ALL FRUITS OF WARRANTLESS SEARCHES  
CONDUCTED FROM JANUARY 4, 2011, TO JANUARY 6, 2011,  
AND INCORPORATED MEMORANDUM OF LAW  
(MOTION TO SUPPRESS NO. 2)**

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case all evidence derived from unlawful warrantless searches of, and unlawful interceptions of electronic communications/data to and from, an ACER netbook belonging to him, from January 4, 2011, through January 6, 2011, and all derivative fruits thereof.

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his netbook and in the communications/data flowing to and from it.<sup>1</sup>

2. From January 4, 2011, through January 6, 2011, MIT personnel, Secret Service agents, and Cambridge police unlawfully searched his ACER netbook and intercepted communications/data flowing to and from the netbook, without either a search warrant or an order authorizing the interception of electronic communications under Title III.

3. To the extent that such searches/interceptions were carried out by MIT personnel, they were acting as government agents, and the requirements of the Fourth Amendment apply.

---

<sup>1</sup> All averments herein regarding Swartz's ownership and possession of the ACER laptop and the hard drive are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

4. The evidence, along with all derivative fruits thereof, must, therefore, be suppressed.

**THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.**

**LOCAL RULE 7.1(A)(2) STATEMENT**

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

**MEMORANDUM OF LAW**

**I. FACTUAL BACKGROUND.**

From September 27, 2010, until January 4, 2011, MIT personnel conducted an investigation into the downloading of large quantities of material from JSTOR, an online archive which provides access to academic journals.<sup>2</sup> Timeline of events related to JSTOR downloading incident: 9/26/10-1/6/11 ("Timeline"), Exhibit 1 at 1-5. On January 4, 2011, Dave Newman, MIT Senior Network Engineer, located an ACER netbook in a data room in the basement of an MIT building, which Newman believed was the computer being used to download journal articles from JSTOR. Timeline at 6. Newman, in consultation with Paul Acosta, MIT Manager of Network Operations, decided to leave the netbook physically undisturbed and instead to institute a "capture" of the network traffic to and from the netbook, which was done via Newman's laptop, which was connected to the netbook and which intercepted communications coming to it. *Id.*; US Secret Service Investigative Report ("Investigative Report"), Exhibit 15 at 2. These interceptions were commenced without a warrant or other judicial process. At 11:00 am, Captain Jay Perault of the MIT police arrived, along with

---

<sup>2</sup> The events which occurred during this time period are further addressed in a separate motion to suppress. *See* Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law. The events relevant to this motion began on the morning of January 4, 2011.

Det. Joseph Murphy of the Cambridge Police Department and Secret Service S/A Michael Pickett, who told MIT personnel that he handled computer forensics for the Secret Service. *Id.*; Investigative Report at 1. It was decided, “*at the recommendation of Michael Pickett,*” that the netbook would be left in place, with MIT continuing to monitor the traffic to and from it, and that video surveillance would be set up in the data room to assist in identifying “the suspect.” Timeline at 6 (emphasis added). See Grand Jury Testimony of Det. Joseph Murphy, July 14, 2011, Exhibit 16 at 66 (“Murphy Grand Jury”)(Murphy testified that after learning that MIT had begun the packet capture, “we” told MIT personnel that “[w]e’d like you to keep this running” and, ultimately, “we end up persuading them to leave that on the system”); Email from Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, to Ann Wolpert, MIT Director of Libraries, January 4, 2011, 3:35 pm, Exhibit 17 (“the offending computer has been found, on the MIT campus. *The police would like to leave it up and running for a couple of days while the investigation continues*” (emphasis added)). Neither S/A Pickett nor Det. Murphy applied for or received a Title III warrant authorizing the interception of electronic communications or were in any way authorized by judicial process to direct and persuade MIT personnel to intercept communications and other data flowing to and from the ACER netbook between 11:00 am on January 4, 2011, and the time of the seizure of the ACER on January 6, 2011.

During the morning of January 4, 2011, the search participants observed that “the netbook [was] still reaching out to JSTOR and downloading journals.” *Id.* A warrantless NMap search<sup>3</sup> of the netbook showed that ports 22 and 8092 – ports associated with remote access – were open. Timeline at 7; Investigative Report at 1. The laptop was also physically manipulated and

---

<sup>3</sup> NMap is a sophisticated port-scanning software that can determine a large amount of information about a computer, including which of a computer’s ports are open, the computer’s operating system, and which of thousands of services and protocols the computer is using. See <http://en.wikipedia.org/wiki/Nmap> (last visited Sept. 19, 2012).

fingerprinted without a warrant by law enforcement officers. The outside of the netbook was examined, including picking it up and manipulating it. *See* Exhibit 18. The netbook was opened, and the computer screen which showed the operating system being used and the log-in screen which showed a computer name of "ghost-laptop" with the user name "Gene Host" were accessed and photographed. *See* Exhibit 19. The log-in screen required a password, and all efforts to bypass it were unsuccessful. Email from S/A Pickett to AUSA Adam Bookbinder, January 5, 2011 ("Pickett 1/5/11 email"), Exhibit 20 at 1. In addition, the closed, hard-shell case containing the hard drive was fingerprinted; the case was opened, and the hard drive, which law enforcement believed was being used to store the downloaded data, was examined and separately finger printed. *See* Exhibit 21. The opening of the hard drive case and examination of the case and its contents were all done by law enforcement officers on January 4, 2011, without a warrant or any other judicial process.

Newman, Acosta, and S/A Pickett, along with Mike Halsall, MIT Senior Network & Information Security Analyst, continued to physically monitor the netbook until 2:30 pm. Timeline at 7. During that time "strategy [was] determined for continual monitoring of traffic to/from the netbook." *Id.* After the MIT General Counsel's office approved the disclosure of information to law enforcement agents even in the absence of a warrant or process complying with the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.* (and in contravention of MIT's published policies of only disclosing such information after receipt of such process), and at a time when MIT personnel were acting as government agents, Halsall gave S/A Pickett historical network flow data relating to two IP addresses associated with the netbook from December 14, 2010, up to that date,<sup>4</sup> and DHCP log information for computers using the MIT network as "ghost macbook" and "ghost

---

<sup>4</sup> Network flow data shows connections made between computers and the amount of information transmitted. It shows the start and stop time of a connection, the source IP address, the IP address of the website contacted, source and destination port numbers, and the number of bytes of information transmitted.

24 at 2. Those same notes stated that it was “now a Federal case” and that everything that had been provided was done “by choice,” and not pursuant to a subpoena. *Id.* at 3. Also on January 5, 2011, Newman emailed S/A Pickett at 5:02 pm, stating: “I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads. . . *I was just wondering what the next step is.*” Exhibit 25 (“Email chain”) at 2 (emphasis added).<sup>7</sup> The next morning, January 6, 2011, at 9:37 am, Perault sent an email to Newman, S/A Pickett, and Det. Murphy suggesting that the netbook and hard drive be taken offline and asking if the hard drive should be “printed,” i.e., imaged. *Id.* S/A Pickett responded, agreeing that the netbook should be taken offline and imaged. *Id.* However, he recommended that the video surveillance be maintained because he believed that whoever was using it would return once he noticed that the netbook was offline. Email chain at 1. There was no consideration in any email or report of seeking a judicial warrant for the ongoing interceptions of communications that were being diverted onto and copied on Newman’s computer or any consideration of whether judicial process was required for the real-time monitoring of MIT’s DHCP logs to identify whether and when the ACER netbook was moved or its connection to the MIT network altered. Given the ongoing video surveillance of the laptop – and the known practice of the owner to return to the data room to swap external hard drives – it cannot be contended that the purpose of the ongoing interceptions of data or the decisions to image the ACER were made to identify the owner rather than for purely law enforcement purposes.

At 12:32 pm on January 6, 2011, an individual later identified as Swartz was observed via video surveillance to enter the data room, remove the netbook and hard drive, and place them in his backpack. Timeline at 7; Investigative Report at 3. Swartz was arrested shortly thereafter; his

---

<sup>7</sup> The network traffic being intercepted and copied without a warrant was the content of the data or emails or communications between the ACER netbook and third parties, including, but not limited to, JSTOR.

backpack was searched, but the netbook was not there. Investigative Report at 3. When Halsall checked the DHCP logs for computer registrations using the word "ghost" later that afternoon, he observed that the netbook was still active on the MIT network using the same MAC address it had used on January 4, 2011. The netbook was traced to the fifth floor of the Student Center. S/A Pickett was notified and met Halsall at the Student Center. They located the netbook and external hard drive neatly placed under a table, connected to the MIT network. S/A Pickett examined the netbook, which appeared to be frozen halfway in the shutdown state. Attempts were made by the Secret Service to access a terminal on the machine but were unsuccessful; "[i]t 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." Investigative Report at 3. The laptop and hard drive were again fingerprinted on January 6, 2012. The laptop and hard drive were then seized and turned over to MIT police. Timeline at 10; Investigative Report at 3. In a January 8, 2011, email from Halsall to Mark Sillis, Halsall's supervisor, discussing Swartz's movements on January 6, 2011, Halsall stated that he had been "gathering up all the stuff for Pickett." Exhibit 26. In a separate email from Halsall to S/A Pickett on January 8, 2011, Halsall told Pickett that he "hop[ed] to have the pcap/flows/videos/logs all in by to me Monday, possibly sooner – if you don't already have a copy of the video or pcap [packet capture], I'll make sure you get one." Exhibit 2.

At no time before or during these events was Title III authorization sought for the interception of electronic communications to or from the netbook. No warrant (not even a "sneak and peek" warrant pursuant to 18 U.S.C. §3103a which would have preserved the secrecy of the ongoing efforts to identify the owner of the netbook) to search the netbook or the external hard drive, both of which were seized on January 6, 2011, was obtained until February 9, 2011. Even then, the warrant was not executed, necessitating a reapplication for a search warrant, which was again issued



on February 24, 2011.

**II. SWARTZ HAD A REASONABLE EXPECTATION OF PRIVACY IN THE NETBOOK AND EXTERNAL HARD DRIVE.**

"Courts routinely recognize that individuals possess objectively reasonable expectations of privacy in the contents of their computers." *United States v. Howe*, 2011 WL 2160472 at \*7 (W.D.N.Y. May 27, 2011), adopted 2012 WL 1565708 (W.D.N.Y. May 1, 2012). "Expectations of privacy in the contents of a computer are likened to expectations of privacy in other types of containers, such as suitcases or briefcases. . . . 'Because intimate information is commonly stored on computers, it seems natural that [personal] computers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy.'" *United States v. Trejo*, 2010 WL 940036 at \*4 (E.D.Mich. March 12, 2010), *aff'd* 471 Fed. Appx. 442 (6th Cir. 2012), quoting *United States v. v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007). "Whether a defendant has a reasonable expectation of privacy in a particular place is a two-pronged inquiry. [The Court] consider[s] first, whether the movant has exhibited an actual, subjective, expectation of privacy; and second, whether such subjective expectation is one that society is prepared to recognize as objectively reasonable." *United States v. Werra*, 638 F.3d 326, 331 (1st Cir. 2011). Both of these requirements are amply satisfied here.

The netbook and hard drive belonged to Swartz, and he took pains to place the netbook and hard drive in locations in which they would be free from interference by outsiders, first in a basement data room which appeared from the outside to be locked, concealed under a box, Timeline at 6; Murphy Grand Jury at 82-83, and then under a table in a private area of the Student Center. Critically, the computer was password protected to prevent access to its contents. *See, e.g., United States v. Reeves*, 2012 WL 1806164 at \*8 (May 17, 2012)(fact that defendant's computer was password protected was "sufficient to show her intent to exclude members of the public and maintain

privacy in the documents kept on her computer"); *Clements-Jeffrey v. City of Springfield*, 2011 WL 3207363 at \*3 (S.D. Ohio July 27, 2011)("Personal computers that are password protected are subject to even greater privacy protection"); *United States v. Griswold*, 2011 WL 7473466 at \*12 (W.D.N.Y. June 2, 2011)("In this age of electronically stored information a reasonably well trained police officer should know that an individual's use of a password to protect against unauthorized access to electronic files stored on his or her computer is no less an indication of personal privacy than the use of a lock and key by the owner of a file cabinet"); *Howe*, 2011 WL 2160472 at \*7 (defendant's use of a password to protect the files on the computer demonstrates his subjective expectation of privacy in the contents); see also *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001)(co-user of computer could not validly consent to search of defendant's password-protected files on the computer to which co-user did not have access). Swartz plainly had a subjective expectation of privacy in the netbook and the external hard drive.

That expectation, moreover, is one which society should recognize as objectively reasonable. The netbook was connected to the MIT network, but "the mere act of accessing a network does not in itself extinguish privacy expectations." *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). MIT has a liberal guest access policy, which was described by Tim McGovern, MIT Manager of Network Security & Support Services, as follows:

No authentication of visitors. Visitor network access is provided as an on-demand self-service process for anyone who walks onto campus, plugs in, or elects to use our wireless network, and declares themselves a visitor, and they get 14 days of network privileges.  
No identity verification. Visitors are asked to provide an email address. The email address is not used to verify that a bona fide identity exists . . . .  
No authentication of users accessing JSTOR.org. By agreement, JSTOR.org allows any computer with a net 18 IP address [an MIT IP address] to access their resources without further identification or authentication.

Exhibit 3. Nothing on the MIT website relating to guest use of the MIT network diminishes this legitimate expectation of privacy. Nothing on the MIT website precludes guests – or students or

faculty members – from leaving their laptops in private areas of the campus while downloading data from the internet.

Contrary to the government's argument in its Response to Defendant Aaron Swartz's Motion for Discovery (Doc. 41) at 6, Swartz did not forfeit his expectation of privacy in his netbook and external hard drive because he was a trespasser; those items remained closed containers which were his personal property and which were not abandoned, *see* pages 11-12, *infra*. Swartz was not a trespasser at MIT in any sense. The MIT campus is not closed to persons other than students, faculty, and employees. On the contrary: it is an open campus with practices that encourage persons who are members of the broader Cambridge technical community to share its resources. Swartz has lectured to an MIT class, audited classes at MIT, worked on projects with MIT professors, and has been a valued member of MIT forums and groups.

The cases on which the government relied are uniformly inapposite. In *United States v. Terry*, 2007 WL 496630 (S.D.Ga. Feb. 12, 2007), *aff'd* 258 Fed. Appx. 304 (11th Cir. 2007), the defendant appropriated to himself a unit in a storage facility which he did not rent and had no right to occupy and affixed a padlock to it. Similarly, in *United States v. Pitt*, 717 F.2d 1334 (11th Cir. 1983), the defendant padlocked a room belonging to his girlfriend's landlady, to which his girlfriend, as the tenant, had no right of access or use, and which the landlady had reserved to her exclusive use. In *United States v. Hightower*, 1987 WL 44897 (6th Cir. Sept. 28, 1987), the defendant placed locks on country club lockers which he was not authorized to use and for which he had not paid the required fee. In *United States v. Sanchez*, 635 F.2d 47 (2d Cir. 1980), the defendant was unable to demonstrate ownership of or authority from the owner to possess and use the automobile which was the subject of the challenged search. What *Sanchez* says is that "a mere trespasser has no Fourth Amendment protection *in premises* he occupies wrongfully." *Id.* at 64 (emphasis added). Like the

other cases on which the government relied, *Sanchez* involved an assertion of a reasonable expectation of privacy in the entire premises at issue – the storage unit, the landlady’s storage room, the car, the lockers – which is not the issue here. Swartz does not suggest that he had a reasonable expectation of privacy in the data room, but solely in his private property located therein – the netbook and the external hard drive -- and in the electronic communications to and from his netbook. The data room was located within a network of hallways which were used by people to travel between MIT buildings, especially in the winter. Murphy Grand Jury at 82-83. There were classrooms on the same floor, and students used the corridor to attend classes. There were no signs ordering people to keep out, *see* Exhibit 27, and the door to the data room opened readily with a “quick jerk.” Murphy Grand Jury at 84. Swartz simply was not a trespasser in the sense which led to the decisions in *Sanchez* and the government’s other cases. *See United States v. Scott*, 673 F.Supp.2d 331, 339 (M.D.Pa. 2009)(defendant had reasonable expectation of privacy in computer belonging to him seized from apartment where defendant did not contend that he lived or stayed for any period of time or that he was ever invited to the apartment or that he had a key to the apartment).

Nor did Swartz abandon the netbook. To find abandonment, there must be “clear and unequivocal evidence” that the defendant intended to abandon the property. *United States v. Crist*, 627 F.Supp.2d 575, 580-81 (M.D.Pa. 2008)(holding that defendant did not abandon computer where he returned to house to get it 26 days after his rent became overdue, eviction proceedings had not commenced, and defendant had received no notice that his property would be removed), *quoting United States v. v. Fulani*, 368 F.3d 351, 354 (3d Cir. 2008). Here, Swartz neither denied ownership of the netbook nor physically relinquished the item. *See United States v. James*, 353 F.3d 606, 615-16 (8th Cir. 2003)(defendant did not abandon computer disks he gave to a friend to store, even after he told the friend to destroy them); *United States v. Upham*, 168 F.3d 532, 357 (1st Cir.

1999)(defendant did not abandon computer images by deleting them); *United States v. Infante-Ruiz*, 13 F.3d 498, 501-02 (1st Cir. 1994)(defendant did not repudiate privacy interests by leaving his unlocked briefcase in the locked truck of another person's car, even though he allowed other people to store items in it because "he did nothing to indicate its availability to the public generally nor did his actions betray an intention to forego an owner's normal right to exclude those he wished to exclude"). Notably, the law enforcement officials on the scene did not believe that the netbook was abandoned, as they set up video surveillance in anticipation of the owner's return, and, indeed, Swartz was observed returning to the netbook on the afternoon of January 4, 2011, and on January 6, 2011.

The netbook and external hard drive were seized from the Student Information Processing Board Office, a small private office located in the MIT student center, *i.e.*, it was not seized from the Building 16 data closet. A student who was present when Swartz entered the room, and whose identity is known to the government, told Cambridge Police that Swartz asked permission to use a network drop in the room, and the student pointed him to one. After the student told Swartz that he was leaving and needed to lock the room, Swartz left, as did the student, locking the door behind him. Thus, Swartz had the permission of a person with authority over the room (as evidenced by his possession of keys to it) to connect to the MIT network in the room and had every reason to believe that the netbook was in a private, locked space where it would remain unmolested. He had both a subjective and objectively reasonable expectation of privacy in the netbook and hard drive.

### **III. THE SEARCHES AT ISSUE HERE.**

#### **A. The January 4, 2011, and January 6, 2011, External Examination and Fingerprinting of the Netbook and Hard Drive.**

While the netbook and external hard drive were in plain view, and law enforcement officers were lawfully on the premises, the physical manipulation of the netbook and external

hard drive by law enforcement personnel to examine its external attributes and to fingerprint it constituted a warrantless search within the meaning of the Fourth Amendment. *See, e.g., Arizona v. Hicks*, 480 U.S. 321, 324-25 (1987)(officer's moving of turntable to examine its exterior constituted Fourth Amendment search). As the Supreme Court explained in *Hicks*: "[T]he distinction between 'looking' at a suspicious object in plain view and 'moving' it even a few inches is much more than trivial for purposes of the Fourth Amendment. It matters not that the search uncovered nothing of any great personal value to respondent – serial numbers rather than (what might conceivably have been hidden behind or under the equipment) letters or photographs. A search is a search, even if it happens to disclose nothing but the bottom of a turntable." *Id.* at 325. *See, e.g., United States v. Paneto*, 661 F.3d 709, 714 n.3 (1st Cir. 2011)("Under *Hicks*, it is clear that the Fourth Amendment forbids handling an item to expose something hidden"). The same reasoning applies with equal force to the opening of the hard drive case and the examination of the hard drive contained within it. The fruits of the external examination of the netbook and the external hard drive and its case must, accordingly be suppressed.

**B. The Internal Examination of the Netbook.**

The opening of the netbook, the observation of the screen showing the operating system in use and the log-in screen, the attempts to bypass the log-in screen, and the conducting of an NMap search of the netbook to determine which ports were open, constituted a search within the meaning of the Fourth Amendment. *See, e.g., United States v. Musgrave*, 845 F.Supp.2d 932, 949 (E.D.Wis. 2011)(touching key or moving mouse to expose screen that was not previously in view is Fourth Amendment search); *United States v. Crist*, 627 F.Supp.2d 575, 585 (M.D.Pa. 2008)(running of hash values is a Fourth Amendment search); *see also United States v. Phillips*, 477 F.3d 215, 217 (5th Cir. 2007)(describing port scanning as "the

electronic equivalent of 'rattling doorknobs' to see if easy access can be gained to a room"). The internal examination of the laptop and its functions was a search, just as opening a locked briefcase or file cabinet and examining its contents is, and could not lawfully be conducted in the absence of a search warrant duly issued upon a showing of probable cause. The fruits of this internal examination must, accordingly, be suppressed.

**C. The Capture of Electronic Communications to the Netbook.**

18 U.S.C. §2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce . . . ." Section 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." "Contents" is in turn defined as "any information concerning the substance, purport or meaning" of the communication. §2510(8). The "packet capture" which MIT continued to undertake at the recommendation of S/A Pickett and the persuasion of Det. Murphy captured the entire communication, including subject matter and content. That it intercepted the content of electronic communications is obvious from Newman's January 5, 2011, email to S/A Pickett informing him that he had "collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads." Email chain at 2. Even accepting Newman's calculations, that means that 2% of the 70G of intercepted data, communications, emails, and the like, involved parties other than JSTOR, *see, e.g.*, Exhibit 28 (showing interception of communications of third party), a significant violation of the Fourth Amendment, as was the warrantless seizure of the 98% of the content emanating, according to Newman, from JSTOR. Obviously, Newman, working in concert with S/A



Pickett, must have searched his copy of the intercepted communications to make his numerical assessment. Use of the packet capture constituted the interception of electronic communications within the meaning of Title III, *see, e.g., United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*)(diverting incoming communications constitutes interception within the meaning of Title III), which was unlawful in the absence of a valid order authorizing the interceptions of the electronic communications, of which none were sought or issued here.

None of the exceptions to the prohibition of warrantless interception of electronic communications are applicable here. Section 2511(2)(a)(i) provides:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights and property of the provider of that service . . . .

This section is inapplicable here because, as more fully addressed in the next section of the memorandum, MIT personnel were acting as government agents beginning no later than 11:00 am on January 4, 2011, and the packet capture was conducted by them as government agents. Because they were acting as government agents, "the requirements of the Fourth Amendment . . . override statutory authority." *United States v. Pervaz*, 118 F.3d 1, 5 (1st Cir. 1997). *See McClelland v. McGrath*, 31 F.Supp.2d 616, 618 (N.D. Ill. 1998)("What the officers do not seem to understand . . . is that *they* are not free to ask or direct Cellular One to intercept *any* phone calls or disclose their contents, at least not without complying with the judicial authorization provisions of the Wiretap Act, *regardless* of whether Cellular One would have been entitled to intercept those calls on its own initiative" (emphasis in original)); *United States v. Auler*, 539 F.2d 642, 647 (7th Cir. 1976)("Government agents must not rely on telephone company employees to act on their behalf

without complying with the requirements of the Fourth Amendment. . . . In no situation may the Government direct the telephone company to intercept wire communications in order to circumvent the warrant requirements of a reasonable search"); *United States v. Hudson*, 2011 WL 4727811 at \*3 (E.D.La. Oct. 5, 2011) ("If the Alltel employees were government agents, . . . they would not satisfy the carrier exception of Title III, and their conduct would be judged under the standards of the Fourth Amendment").<sup>8</sup>

This conclusion is reflected in the USDOJ manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, which instructs that the provider exception "does not permit law enforcement officers to direct or ask system administrators to monitor for law enforcement purposes." *Id.* at 174-75. The Manual continues:

After law enforcement and the provider have communicated with each other, . . . the cautious approach is only to accept the fruits of a provider's monitoring if certain criteria have been met that indicate that the provider is monitoring and disclosing to protect its rights or property. These criteria are: . . . (3) law enforcement has not tasked, directed, requested or coached the monitoring for law enforcement purposes, and (4) law enforcement does not participate in or control the actual monitoring that occurs.

*Id.* at 175 (emphasis added). Here, law enforcement plainly, at a minimum, "requested or coached the monitoring for law enforcement purposes." See *Murphy Grand Jury* at 66 (Murphy testified that after learning that MIT had begun the packet capture, "we" told MIT personnel that "[w]e'd like you to keep this running" and, ultimately, "we end up *persuading* them to leave that on the system" (emphasis added)). The provider exception is, accordingly, inapplicable.<sup>9</sup>

---

<sup>8</sup> MIT's interceptions prior to January 4, 2011, are addressed in a separate motion to suppress. See Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law.

<sup>9</sup> Moreover, §2511(2)(a)(i) has a reasonableness requirement – an electronic communications service provider may intercept communications only insofar as such interception is "a necessary incident" to the protection of its rights and property. See, e.g., *United States v. Harvey*, 540 F.2d

in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests.” *United States v. Pervaz*, 118 F.3d 1, 6 (1st Cir. 1997). *See, e.g., United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008) (“the police must have instigated, encouraged or participated in the search,” and “the individual must have engaged in the search with the intent of assisting the police in their investigative efforts”); *United States v. Souza*, 223 F.3d 1197, 1201-02 (10th Cir. 2000) (Police must “instigate, orchestrate, encourage or exceed the scope of the private search to trigger the application of the Fourth Amendment”); *United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994) (inquiry is “(1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends”); *see also United States v. Van Dyke*, 2010 WL 1949640 at \*3 (W.D.Mich. May 14, 2010) (“permitting the government to circumvent the limits of the Fourth Amendment by directing individuals to conduct searches that the government cannot, would totally undermine the purposes of the Fourth Amendment”).

This standard is plainly met in this case, particularly with respect to the continuing packet capture of electronic communications to Swartz’s netbook and the real-time provision of DHCP log information from January 4, 2011, through January 6, 2011.<sup>10</sup> Once S/A Pickett and Det. Murphy arrived on the scene, it became a law enforcement investigation. Once the netbook was located, no further investigation was necessary to protect MIT’s rights or property. The investigation which began with the arrival of S/A Pickett and Det. Murphy was a law enforcement investigation with the object of identifying, arresting, and prosecuting the individual responsible for the downloads from

---

<sup>10</sup> *See* Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law.

JSTOR. The netbook was left in place, with MIT continuing to monitor it at the recommendation of S/A Pickett and upon the urging of Det. Murphy. *See* page 3, *supra*. The monitoring strategy was developed in consultation with S/A Pickett and Det. Murphy. The monitoring was continued because law enforcement wanted to gather evidence of intent and motive, *see* page 6, *supra*, matters of no relevance whatsoever to the protection of MIT's interests. MIT recognized on January 4, 2011, that "[t]he investigation ha[d] moved beyond MIT was [was] now being handled by law enforcement." Exhibit 22. MIT personnel asked S/A Pickett on January 5, 2011, "what the next step [was]," Exhibit 25, further illustrating S/A Pickett's direction of the investigation. Halsall admitted that he was "gathering up all the stuff for Pickett." Exhibit 26. MIT personnel asked S/A Pickett's permission before taking the netbook offline and asked him whether they should image the netbook. *See* page 6, *supra*. In an email from Halsall to S/A Pickett on January 8, 2011, Halsall told Pickett that he "hop[ed] to have the pcap/flows/videos/logs all in by to me Monday, possibly sooner – if you don't already have a copy of the video or pcap [packet capture], I'll make sure you get one." Exhibit 2.

Here, the government plainly encouraged the search, played a role in its design and operation, and MIT personnel deferred to the guidance of law enforcement officers, aiming to assist the government in its criminal investigation rather than being motivated by its own interests. Beginning with the arrival of S/A Pickett and Det. Murphy on January 4, 2011, MIT personnel were acting as government agents, and the requirements of the Fourth Amendment are fully applicable to any search or interception of electronic communications conducted by them. These interceptions were unlawful in the absence of a warrant, issued upon a showing of probable cause. The intercepted communications, as well as all derivative fruits thereof, must be suppressed.

Respectfully submitted,  
By his attorney,

/s/ Martin G. Weinberg

Martin G. Weinberg  
20 Park Plaza, Suite 1000  
Boston, MA 02116  
(617) 227-3700 (tel.)  
(617) 338-9538 (fax)  
owlmgw@att.net

**CERTIFICATE OF SERVICE**

I, Martin G. Weinberg, hereby certify that on this 5th day of October, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA. One copy of the exhibits to the motion was served on the government by hand this same date.

/s/ Martin G. Weinberg

Martin G. Weinberg

[For Faculty & Staff](#) [For Students](#) [For IT Support Providers](#)



[GET STARTED  
WITH IT](#)

[OUR  
SERVICES](#)

[SOFTWARE  
& HARDWARE](#)

[SECURE  
COMPUTING](#)

[ABOUT  
IS&T](#)

## IS&T Policies: DHCP Usage Logs Policy

[About IS&T](#) > [IT Policies](#) > [IS&T Policies: DHCP Usage Logs Policy](#)

[Get Help](#)

### On this page:

[Policy](#)

[Rationale](#)

[Implementation](#)

[Implications](#)

[Glossary](#)

[History](#)

### Policy

IS&T records a variety of information about both the operation and/or use of its network services. When used in conjunction with IS&T's Host Registration database, records contained in logs showing the use of dynamic IP addresses on MITnet allow IS&T staff to follow up on problems, incidents, and inquiries.

These logs are retained for 30 days after their creation date. All of these logs are considered confidential, and as such IS&T takes active measures to prevent unauthorized access during the retention period.

Circumstances may arise where a log, or more usually a very small subset of one day's log, may need to be kept for longer than 30 days and, potentially, disclosed to certain third parties. The use of any such retained information by authorized staff, and the release of any log information to third parties, are done under the direction and with the approval of MIT's Office of the General Counsel.

This IS&T policy is limited to the Dynamic Host Configuration Protocol (DHCP) services and logs created in connection with MITnet. It does not apply to DHCP services or logs created by other Departments, Labs & Centers (DLCs) at MIT. IS&T recommends that other IT groups at MIT create similar policies that are based on business practices and are consistent with the needs and desires of those DLCs.

## Rationale

This policy implements MIT's Privacy Policy specifically for the collection and retention of DHCP logs. In setting the retention period, IS&T has weighed a variety of competing interests, chiefly the need to maintain robust operational reliability of MIT's network, the need to be responsive to third parties who report issues that we need to investigate or resolve, and the desire to limit log retention to reduce opportunities for inadvertent disclosure of operational data.

## Implementation

The DHCP server is configured to provide dynamic addresses automatically as needed. The logs of information are maintained on an IS&T-managed server. Each log is tagged with its creation date; once a day, the system deletes logs that are 30 days old.

When any network device, e.g., a computer, connects to MITnet and is assigned a dynamic IP address, MIT's DHCP server adds a record to its log containing the following information:

- The date and time of the request
- The MAC address of the requesting device or computer
- The IP address provided
- The specific DHCP command that was issued
- Other technical information related to the request

In the event of a request relating to a potential legal proceeding, IS&T staff may create a case in Request Tracker and store subsets of a log pertinent to the case at hand in the case record.

The DHCP server is in a secure location and complies with secure data storage best practices. IS&T's Network Services Infrastructure team acts as the data custodian for DHCP logs, and ensures that the logs are stored securely and are deleted when they expire.

The DHCP logs capture only one type of network usage. Related, but not addressed in this policy, are Virtual Private Network (VPN) usage logs, hostnames/static IP addresses usage logs, or dialup usage logs, among others.

## Implications



Retaining and securing DHCP usage logs as described above are necessary to ensure that the confidentiality of the DHCP lease logs is protected but that the information in the logs is still available as needed to ensure MITnet's security and integrity.

MIT is required to comply with a court order or valid subpoena that requests the disclosure of information contained in DHCP logs. Failure to comply could have serious consequences for the individuals, IS&T, and the Institute. MIT's Office of the General Counsel is qualified and authorized to confirm that a request for information contained in logs is legitimate and not an improper attempt to gain access to confidential information.

## Glossary

**DHCP:** Dynamic Host Configuration Protocol. This protocol defines the process by which a device can dynamically receive an IP address from a pool of addresses, instead of requiring the device to have a fixed IP address. This is ideal for devices like laptops, which will not all be connected to the network at all times from the same location.

**Dynamic IP Address:** When a device has not been assigned a Static IP address, an Internet service provider will assign an address at the time the device is connecting to the Internet.

**IP Address:** Internet Protocol (IP) Address. See references below for more information on network addressing.

**DLCs:** A collective term meant to describe the common elements among MIT's many academic, administrative and research units, while acknowledging the many differences amongst MIT units.

**Static IP Address:** A number (in the form of a dotted quad) that is assigned to a network device or computer by an Internet service provider (ISP) which will be its permanent address on the Internet.

**VPN:** Virtual Private Network. A technology that in MIT's usage facilitates secure communications from remote locations to a known location at MIT, typically over the public Internet. However, VPNs are not inherently about security or performance, but rather that they provide a "tunnel" on top of some other network in support of a given customer or client community.

## History

**Status:** In effect

**Policy Steward:** Paul Acosta

**Policy Owner:** Marilyn T. Smith

**RELATED PAGES AND HOW  
TO**

IT Policies

Virtual Private Network (VPN)

MITnet Bootstrap Registration

MIT Privacy and Disclosure of  
Information Policy

---

**ABOUT IS&T**

---

**NEWS**

---

**OUR ORGANIZATION**

---

**MISSION & STRATEGIC PLAN**

---

**IT POLICIES**

---

**IT GOVERNANCE**

---

**JOB OPENINGS**

---

Massachusetts  
Institute of Technology

Information Services and Technology |  
617.253.1101  
Ask the Help Desk or contact the IS&T  
Webmasters.

---

**FOR FACULTY & STAFF**

---

**FOR STUDENTS**

---

**FOR VISITORS**

---

FOR IS&T STAFF

---

FOLLOW US

---

Case/Case Name: 01-07-2011 09:00 AM

Version: 3.1.1000

<b>CRIMINAL COMPLAINT</b> <b>ORIGINAL</b>		<b>DOCKET NUMBER</b> 1153CR000073	<b>NO. OF COUNTS</b> 1	<b>Trial Court of Massachusetts</b> <b>District Court Department</b>
<b>DEFENDANT NAME &amp; ADDRESS</b> Aaron H Swartz 349 Marshman Ave. Highland Park, IL 60035				<b>COURT NAME &amp; ADDRESS</b> Cambridge District Court 4040 Mystic Valley Parkway Medford, MA 02155 (781)308-2710
<b>DEFENDANT DOB</b> 11/08/1985	<b>COMPLAINT ISSUED</b> 01/07/2011	<b>DATE OF OFFENSE</b> 01/04/2011	<b>ARREST DATE</b> 01/06/2011	<b>ARREST</b>
<b>OFFENSE CITY / TOWN</b> Cambridge		<b>OFFENSE ADDRESS</b>		
<b>POLICE DEPARTMENT</b> MIT Campus Police		<b>POLICE INCIDENT NUMBER</b> 11000351		<b>NEXT EVENT DATE &amp; TIME</b> 01/07/2011 9:00 AM
<b>OSTN</b> TCAM201100032				<b>NEXT SCHEDULED EVENT</b> Arraignment
				<b>ROOM / SESSION</b> Arraignment Session
The undersigned complainant, on behalf of the Commonwealth, on oath complains that on the date(s) indicated below the defendant committed the offense(s) listed below and on any attached pages.				

COUNT	CODE	DESCRIPTION
1	288/1A/B	BAE BUILDING DAYTIME FOR FELONY c286 §16

On 01/04/2011 did in the day time break and enter a ship, motor vehicle or vessel, the property of MIT & Jeter.com, with intent to commit a felony, in violation of G.L. c.288, §16.

PENALTY: state prison not more than 10 years; or jail not more than 2 years and not more than \$500. District Court has final jurisdiction under G.L. c.218, §28.

<b>SIGNATURE OF COMPLAINANT</b> X <i>[Signature]</i>	<b>SWORN TO BEFORE CLERK-MAGISTRATE/CLERK/DEF. ASST. CLERK</b> X <i>[Signature]</i>	<b>DATE</b> 1-7-11
<b>NAME OF COMPLAINANT</b> Craig A. Martin	<b>CLERK-MAGISTRATE/ASST. CLERK</b> X	<b>DATE</b>

Notice to Defendant: 42 U.S.C. § 3786gg-4(e) requires this notice: If you are convicted of a misdemeanor crime of domestic violence you may be prohibited permanently from purchasing and/or possessing a firearm and/or ammunition pursuant to 18 U.S.C. § 922 (a) (9) and other applicable related Federal, State, or local laws.

227

6174945129 P.002

CAMBRIDGE DISTRICT COURT

OCT-18-2012 13:42

RIF



**INCIDENT # / REPORT #**  
**11000351 / 1**

**OFFICER  
J. PERAULT**

# BANK DETECTIVE

**REVIEW STATUS**  
**APPROVED by JPERAULT**

**INCIDENT #11000351 DATA**

As Of 01/06/2011 16:19:21

## BASIC INFORMATION

**CASE TITLE**  
**B&E**

**LOCATION**  
**21 AMES ST**

# ATLANTA

**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 c256 S18

**PERSONS**

<u>ROLE</u>	<u>NAME</u>	<u>SEX</u>	<u>RACE</u>	<u>AGE</u>	<u>DOB</u>	<u>PHONE</u>
<u>VICTIM</u>	MIT,					(HOME)
	<u>ADDRESS:</u>	[REDACTED]			CAMBRIDGE, MA	(CELL)

## OFFENDERS

<u>STATUS</u>	<u>NAME</u>	<u>SEX</u>	<u>RACE</u>	<u>AGE</u>	<u>DOB</u>	<u>PHONE</u>
DEFENDANT	SWARTZ, AARON H	MALE	UNKNOWN	24	[REDACTED]	(HOME)
	ADDRESS: , IL					(CELL)

**[ NO VEHICLES ]**

**PROPERTY**

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

**OFFICER REPORT: 11000351 - 1 / JPERAULT (DETECTIVE)**

**DATE/TIME OF REPORT**  
01/06/2011 14:00:45

**TYPE OF REPORT**  
**INCIDENT**

**REVIEW STATUS**  
**APPROVED**

## NARRATIVE

On January 4, 2010 at approximately 10:30 hours I responded to MIT building 16, room 004T for a report of a past break. This room is a telephone closet and networking closet; it's access is controlled by MIT's IS&T Department. David Newman of MIT IS&T explained to me that someone had entered the restricted room and connected a laptop and external hard drive directly to a networking switch. The

# RIF

laptop and external hard drive were being hidden under a cardboard box. Newman further explained that they were able to determine that this laptop was illegally downloading scientific periodicals from JSTOR, a subscription based database that houses academic periodicals.

Cambridge Police Detective Joseph Murphy, Special Agent Michael Pickett from the United States Secret Service and Boston Police Officer Tim Laham responded to building 16 room 004T. Cambridge Police's Crime Scene Services also responded and processed the laptop and external hard drive for latent prints. It was determined that the laptop would be left in place and IS&T would monitor the network traffic in an attempt to identify the suspect. A camera was also installed by MIT's IS&T Department to monitor the area.

On January 4, 2010 at approximately 15:26 hours a white male, dark or black shoulder length wavy hair, wearing a dark coat, gray backpack, jeans with a white bicycle helmet enters the room. It appears as though the suspect takes a hard drive out of his back pack and bends over the laptop and external hard drive. He exits the room moments later.

On January 5, 2010 MIT's IS&T Department informed me that approximately 70 gigabytes of data had been downloaded, 98% of which was from JSTOR. SA Mike Pickett had informed me that MIT's IS&T had put an approximate value on the downloaded information at \$50,000.

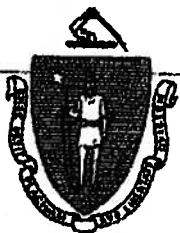
On January 6, 2010 at approximately 12:32 hours a white male, dark or black shoulder length wavy hair, wearing a dark coat, gray backpack, jeans with a white bicycle helmet enters the room. I was monitoring the video feed at the MIT Police Department at this time. It appears as though the suspect packed up the laptop and hard drive and exited the room. MIT Police units responded to the area and searched for the suspect. A check of the room determined that the laptop and hard drive had been removed.

On January 6, 2010 at approximately 14:11 hours Captain Albert Pierce of the MIT Police Department called me and stated he had located the suspect riding his bike on Massachusetts Ave at Lee Street. Special Agent Pickett and I responded to the Lee Street to assist Captain Pierce. The suspect jumped off his bike when encountered by Captain Pierce and ran down Lee Street. Captain Pierce and Special Agent Pickett were able to apprehend the suspect at 24 Lee Street. He was handcuffed by SA Pickett.

The suspect encountered by Captain Pierce and apprehended on Lee Street is the same person seen on video entering the restricted telephone closet in building 16 on January 4th at 15:26 hours and on January 6th at 14:11 hours.

He was arrested for two counts of Breaking and Entering in the daytime with the intent to commit a felony, Chapter 266 Section 1B.

RIF



*The Commonwealth of Massachusetts*

HOUSE OF REPRESENTATIVES  
STATE HOUSE, BOSTON 02139

KENNETH M. LEMANSKI  
8TH HAMPSHIRE DISTRICT

ROOM 445, STATE HOUSE  
TEL. 722-3400

May 24, 1983

Mr. Richard Kendall  
Governor's Legislative Office  
State House - Room 381  
Boston, MA 02133

Dear Mr. Kendall:

Thank you for the opportunity to comment on H.6227, which revises the definition of "property" with respect to larceny.

The most important aspect of this bill, in my opinion, is the fact that it now allows electronic impulses to be defined as property. This is essential in combatting computer crime. As I am sure the Governor is aware, the Commonwealth is extremely dependent on computers of all types, business, academic and so on. H.6227 will give prosecutors what former Senator Ribicoff once called "wiggly room". That is, they will now be able to refer to a specific statute in the prosecution of what was formerly one of the most difficult types of crime. H.6227 directly attacks what, up until now, had been the judicial sticking point: are electronic data "property"? Our own Supreme Judicial Court agreed with earlier Federal opinions that the answer was no, under the existing statutes. H.6227 remedies this by explicitly including computer data in the definition of property.

The second section of H.6227 extends this definition to trade secrets, with the same intent. This is especially important when one stops to think of how much sensitive business data is contained in computers.

The Governor would be taking a great step toward furthering Massachusetts' reputation as a commercially and technologically progressive State by signing H.6227. I urge him most strongly to do so.

Thank you again for this opportunity, and please notify me of any signing.

Sincerely,

A handwritten signature in dark ink, appearing to be "Ken".

Kenneth M. Lemanski  
STATE REPRESENTATIVE

KML/v



**SEARCH WARRANT**  
**HP USB drive,**  
**marked 0045SMKBT1 85102**

**Case No. 11M-5063-JGD**

**RIF**

AO 93 (Rev. 12/09) Search and Seizure Warrant

# UNITED STATES DISTRICT COURT

for the  
District of Massachusetts

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

HP USB drive, marked 0045SMKBT1 85102

Case No.

11M-5863-JGD

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_  
(Identify the person or describe the property to be searched and give its location):  
HP USB drive, marked 0045SMKBT1 85102, as described in Attachment A

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized):  
evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(2), 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1343 (wire fraud,) as described in Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

March 10, 2011

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.

☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Judith G. Dein

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for \_\_\_\_\_ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued:

2/24/11 3:05

City and state: Boston, Massachusetts



Judith G. Dein

Chief U.S. Magistrate Judge Judith G. Dein

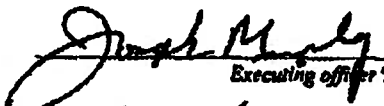
Printed name and title

USAO-000271

232

RIF

AO 93 (Rev. 12/07) Search and Seizure Warrant (Page 2)

Return		
Case No.: <u>11M-5063 JGD</u>	Date and time warrant executed: <u>2/25/2011 9:00 AM</u>	Copy of warrant and inventory left with: <u>Kevin Cavanaugh</u>
Inventory made in the presence of: <u>Property Technician Kevin Cavanaugh &amp; Dep. Sup. Joseph W. Morley</u>		
Inventory of the property taken and name of any person(s) seized:  <div style="margin-left: 40px;"> <p>(1) HP USB Drive</p> <p>marked <del>08</del> 459 MKBT1 85102</p> </div>		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 30%;"> <p>Date: <u>3/4/11</u></p> </div> <div style="width: 60%; text-align: center;">   <small>Executing officer's signature</small>  <u>Joseph Morley Special Fed Dep US Marshal 1</u>  <small>Printed name and title</small> </div> </div>		

**Attachment A**

**HP USB drive, marked 0045SMKBTI 85102**



**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:**
- A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:**
- 1. JSTOR**
  - 2. Massachusetts Institute of Technology**
  - 3. Jstor.org**
  - 4. Mit.edu**
  - 5. IP addresses in the class A domain 18.**
- B. Records and tangible objects pertaining to the following topics:**
- 1. JSTOR**
  - 2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR**
  - 3. Records and data stored on JSTOR**
  - 4. Records and data originating on JSTOR**
  - 5. Means of access to JSTOR**
  - 6. Computer software capable of making repeated requests for data and records from JSTOR**
  - 7. Computer software capable of making repeated downloads of records and data from JSTOR**

8. MIT's computer network
  9. MIT's physical plant
  10. Remote electronic storage locations
  11. MAC addresses
- C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
- D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;
- E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and
- F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
  2. evidence of computer software that would allow remote access and control of the computer equipment
  3. evidence of the attachment of other computer hardware or storage

media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
5. evidence of the times the computer equipment was used;
6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

- II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

#### DEFINITIONS

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,



communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

**ATTACHMENT C**

**PROCEDURES FOR SEIZING COMPUTERS AND RELATED DEVICES**

**1. Seizing hardware and software**

Agents are authorized to seize and remove from the premises the computer hardware, software, related documentation, and storage media, so that computer analysts can accurately retrieve the items authorized by this warrant in a laboratory or other controlled environment. The retrieval process does not need to be completed within 14 days after the date of the warrant or before the return of the written inventory required by Fed. R. Crim. P. 41(a).

**2. Returning hardware and software**

If, after inspecting a seized computer system, the agents and computer analysts determine that these items are no longer necessary to retrieve and preserve electronic evidence, the prosecutor determines that they need not be preserved as evidence, fruits or instrumentalities of a crime, and these items do not contain contraband, they should be returned within a reasonable time, upon written request.

If the computer system cannot be returned, agents should, upon written request, make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that are neither the fruits nor instrumentalities of crime nor contraband.

**APPLICATION FOR  
SEARCH WARRANT**  
HP USB drive,  
marked 0045SMKBT1 85102

**Case No. 11M-5063-JGD**

# UNITED STATES DISTRICT COURT

for the  
District of Massachusetts

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

HP USB drive, marked 0045SMKBT1 85102

Case No. 11M-5063-JED

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

HP USB drive, marked 0045SMKBT1 85102, as described in Attachment A

located in the \_\_\_\_\_ District of \_\_\_\_\_ Massachusetts, there is now concealed (identify the person or describe the property to be seized):

evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(2), 18 U.S.C. § 1030(a)(5)(A) and 18 U.S.C. § 1343 (wire fraud,) as described in Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

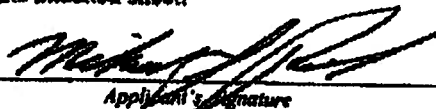
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Sec. 1030(a)(2)	intentionally accessing a computer without authorization and obtaining information
18 U.S.C. Sec. 1030(a)(5)(A)	intentionally causing damage without authorization to a protected computer
18 U.S.C. Sec. 1343	wire fraud

The application is based on these facts:  
See attached Affidavit of Special Agent Michael S. Pickett

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Secret Service Special Agent Michael S. Pickett  
Printed name and title

Sworn to before me and signed in my presence

Date: 2/24/11

City and state: Boston, Massachusetts



  
Judge's signature

Chief U.S. Magistrate Judge Judith G. Dein  
Printed name and title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Michael S. Pickett, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search an Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601 ("the ACER LAPTOP"), a 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675 ("the WESTERN DIGITAL HARD DRIVE"), and an HP USB drive, marked 0045SMKBT1 85102 ("the USB DRIVE"), as described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the United States Secret Service ("the Secret Service"), Department of Homeland Security, and have been since 2003. My current duties include the investigation of electronic crimes and forensic examination of computers and cellular telephones. As an agent, I have participated in numerous investigations involving computer and high technology related crimes, including computer intrusions, Internet fraud and credit card fraud. I also have received specialized training in the investigation of crimes involving unauthorized intrusions into computer networks. In connection with my official responsibilities, I am charged with investigating violations of 18 U.S.C. §§ 1030 and 1343.

3. As set forth herein, there is probable cause to believe that the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE, and the USB DRIVE contain evidence, instrumentalities, and fruits of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud).

4. I make this affidavit based upon communications with witnesses and others with knowledge of the events, conversations with Secret Service agents, Cambridge Police, and MIT police, my review of records gathered in the course of the investigation described below and my

own observations and knowledge. Because this affidavit is intended to show only that there is probable cause for the requested warrants, it does not set forth all aspects of the investigation of which I or other Secret Service agents are aware.

#### **TECHNICAL TERMS**

5. Based on my experience, I use the following technical terms to convey the following meanings for the purpose of this affidavit:

- a. **IP address:** An Internet protocol address (or simply "IP address") is a unique numeric address used by a computer on the Internet. An IP address looks like a series of four numbers, each in the range 0 - 255, separated by periods (e.g., 18.55.7.216). Every computer attached to the Internet must be assigned an IP address so the Internet traffic sent from and directed to that computer may be directed properly from the source to its destination. Most Internet service providers control a range of IP Addresses. The Massachusetts Institute of Technology ("MIT") controls all IP Addresses which begin with the number 18. Some computers have static -- that is, long term -- IP addresses, while others have dynamic -- that is flexibly assigned or frequently changed -- IP addresses.
- b. **MAC address:** A Media Access Control address is a unique identifier assigned to a network interface, in this case, a computer's network interface card. The MAC address most often is assigned by the manufacturer of the network interface card. Although intended to be a permanent and globally unique identification, it is often possible to change the MAC address on hardware, an action often referred to as "MAC address spoofing."

**PROBABLE CAUSE**

6. Based on the facts set forth below, there is probable cause to believe that Aaron Swartz:
- a. broke into a network interface closet at the Massachusetts Institute of Technology ("MIT");
  - b. without authorization, accessed MIT's computer network from a network switch within that closet;
  - c. fraudulently used the appearance of being a MIT student, faculty member or researcher to access JSTOR's extensive electronic library; and
  - d. fraudulently took from that library over a million journal articles which JSTOR made available by paid subscription or individual purchase.

**JSTOR**

7. JSTOR, founded in 1995, is a United States-based, on-line system for archiving and providing access to academic journals. It provides full-text searchable digitized copies of over 1,000 academic journals, dating back for lengthy periods of time. JSTOR is an independent, self-sustaining, non-profit organization.
8. 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 journal titles, JSTOR enables libraries to out-source the storage of these journals, ensures their preservation, and enables authorized users to conduct full-text, cross-disciplinary searches of them.
9. JSTOR licenses all content under copyright from rights holders and gets permission from them both to digitize the content and make the content available online.<sup>1</sup>
10. In the vast majority of instances, JSTOR charges subscription fees to the libraries, universities and publishers who wish to have access to JSTOR's digitized journals. In the

---

<sup>1</sup> Some materials available on JSTOR are not subject to copyright.



instance of a large research university, this annual subscription fee for the various collections of content offered by JSTOR can cost more than fifty thousand dollars. Portions of the subscription fees are shared with the journal publishers who hold the original copyrights. In addition, JSTOR makes available some articles through its Publisher Sales Service, a program offered through participating JSTOR publishers in which journal articles are available for individual purchase. Publishers decide which articles can be purchased and set fees for their articles. JSTOR facilitates the purchase of articles from the archives on behalf of the participating publishers.

#### The Fraudulent Downloads

11. MIT offers short-term service on its computer network to registered campus guests. On September 24, 2010, an individual registered on the network using the pseudonym "Gary Host" and providing the throwaway e-mail address, [ghost@mailinator.com](mailto:ghost@mailinator.com).<sup>2</sup> As part of the registration process, his computer identified the MAC address of its network interface as 00235a735ffb and its client name<sup>3</sup> as "ghost laptop".

12. On September 25, 2010, shortly after midnight, the "ghost laptop" was assigned IP address 18.55.6.215. Later that day, JSTOR experienced an extraordinary volume of automated requests and downloads from its digitized journal collections to that IP address. The downloads continued into the evening, when JSTOR blocked access to its network from 18.55.6.215.

13. The next morning, JSTOR began to experience rapid and voluminous downloads from IP address 18.55.6.216. Accesses from this address continued until the middle of the day, when JSTOR blocked this IP address as well. That day, JSTOR turned to blocking a much

---

<sup>2</sup> Mailinator is a free disposable e-mail address service that allows a user to create a new e-mail address on the fly. Mailinator will accept mail for any mail address within the mailinator.com domain, and allows anyone to read it 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. It is intended to provide users with an anonymous and temporary e-mail address. See <http://mailinator.com/faq.jsp> (Mailinator FAQs), last visited on February 1, 2011.

<sup>3</sup> A computer's name helps to identify it on a network and can be chosen by a user.

broader range of IP address, temporarily denying service to legitimate JSTOR users at MIT.

14. MIT controls the assignment of all IP addresses in which the first block is "18." It has assigned the second block in the IP address for use by specific buildings on campus. In this instance, "18.55" defines connections made to the MIT network from within Building 16 on campus.

15. On September 27, 2010, MIT deactivated the guest registration for the "ghost laptop" by barring the MAC address 00235a735ffb from being assigned a new IP address.

16. On October 2, 2010, "Gary Host," again using a computer with the client name "ghost laptop," registered as a guest and obtained an IP address from the MIT network. He appears to have bypassed the affirmative bar which MIT had placed to his usage of the network by spoofing the MAC Address of the "ghost laptop," changing the last byte of the MAC address from 00235a735ffb to 00235a735ffc (changing the final "b" to "c"). The "ghost laptop" was assigned IP address 18.55.7.48.

17. On October 8, 2010, the perpetrator, using the same naming conventions as he had for "ghost laptop," obtained a guest registration simultaneously for a second computer on the MIT network. "Grace Host" registered the computer client "ghost macbook," providing the e-mail address ghost42@mailinator.com.<sup>4</sup> The MIT network assigned the "ghost macbook" IP address 18.55.5.100, locating the "ghost macbook's" network connection somewhere within Building 16.

18. Extraordinary downloading of JSTOR's digitized copies of journals began just before 3:00 p.m. on October 9, 2010, from IP address 18.55.5.100 (assigned to the "ghost macbook") and continued until approximately 7:00 p.m. In parallel, extraordinary downloading from JSTOR's collections to IP address 18.55.7.48 (assigned to the "ghost laptop") began at approximately 6:30 p.m. and continued as well until approximately 7:00 p.m. that night.

---

<sup>4</sup> The MAC address of the "ghost macbook," 0017f22cb074, is within the range coded by Apple into hardware it manufactures.

19. During the months of November and December, 2010, over two million illegal downloads were made from JSTOR to two IP addresses assigned to Building 16 at MIT; 18.55.6.240 and 18.55.7.240. Of these, approximately half were research articles, with the remainder being reviews, news, editorials, and miscellaneous things. This is more than one hundred times the number of downloads by all the legitimate MIT JSTOR users combined during the same period.

20. JSTOR did not spot this phase of illegal downloading until Christmas time. MIT's network logs reflect that the computer assigned IP address 18.55.6.240 had not registered as a guest on the MIT computer network on this occasion. An analysis on January 4, 2011, however, reflected that both IP addresses 18.55.6.240 and 18.55.7.240 were assigned to a computer with the MAC address 004ce5a0c756. Using network tools available to MIT on this occasion, the computer was tracked back to a specialized network wiring closet in the basement of Building 16 at MIT.

21. There, MIT personnel found, and subsequently showed to law enforcement personnel, the ACER LAPTOP and an external Samsung hard drive, both of which had been concealed under a cardboard box. The laptop had been connected directly into MIT's computer network and the perpetrator had assigned to himself the IP addresses 18.55.6.240 and 18.55.7.240.

22. On January 4, 2011, MIT placed a video camera in the wiring closet. Later that day, the perpetrator, subsequently identified as Aaron Swartz, was videotaped entering the wiring closet. While there, he appeared to replace the external hard drive attached to the laptop.

23. Swartz, who is neither a student nor an employee of MIT, was recorded again entering the wiring closet on January 6, 2011. Before law enforcement officers could get there, he had removed his computer equipment from the closet and left.

24. Later, during the afternoon of January 6, 2011, the laptop removed from the network wiring closet (identified by its MAC address 004ce5a0c756) was plugged into a network

jack in Building W20. There, it was once again registered through MIT's guest services. When it was, the computer identified itself as "ghost laptop," the same identification provided during the illegal downloads in September and October. The ACER LAPTOP and the WESTERN DIGITAL HARD DRIVE were located and recovered by MIT personnel and law enforcement, without the previously observed external hard drive.

25. An MIT police officer who had seen several pictures taken by the covert camera in Building 16's network wiring closet saw Aaron Swartz on a bicycle near MIT, approximately half an hour after the "ghost laptop" had been connected in Building W20. The officer stopped his car, activated its blue lights and displayed his wallet badge. When he sought to question Swartz, Swartz dropped his bike to the ground<sup>5</sup> and fled. The backpack in Swartz's possession at the time he was caught and arrested minutes later appeared to be the same one he had with him on each occasion he was videotaped in the wiring closet at MIT.

26. In the backpack was the USB DRIVE. From my training and experience and information provided to me by other agents, USB drives are frequently used to store software applications, data and records, including .pdf formatted records such as those that were illegally downloaded from JSTOR. They are also frequently used to transfer records and data between computers or hard drives, such as between those connected in the wiring closet to MIT's network and ones available to Swartz outside.<sup>6</sup>

27. On February 9, 2011, the Court issued warrants to search Swartz's residence at 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 ("the PREMISES"), the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE, and the USB

---

<sup>5</sup> I mistakenly stated in my February 9<sup>th</sup> Affidavit that Swartz dropped his backpack to the ground before fleeing from police. He kept it with him when he fled.

<sup>6</sup> As reflected in paragraphs 17 and 18, above, there were two laptops used in the October 9, 2010, illegal downloads from JSTOR. One identified itself to MIT's network as "ghost laptop." The second identified itself to the MIT's network as "ghost macbook" and provided a MAC address within the range coded by Apple into hardware it manufactures. The "ghost macbook" used in the fraud and thefts has not been recovered yet.

DRIVE. The warrant to search the PREMISES was executed on February 11, 2011. The warrants to search the ACER LAPTOP, the WESTERN DIGITAL DRIVE, and the USB DRIVE were not executed prior to their expiration on February 22, 2011. At the time the warrant was issued for these pieces of electronic equipment, they were secured within the Identification Unit Laboratory of the Cambridge Police Department. Throughout the period of February 9, 2011, to the present, they remained within secure areas at Cambridge Police Headquarters, first in the Identification Unit Laboratory, then in the Evidence/Property Unit.

28. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual

memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

#### CONCLUSION

29. Based on the information described above, I have probable cause to believe that Aaron Swartz has violated 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud).

30. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are contained within the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE and the USB DRIVE.

Sworn to under the pains and penalties of perjury,

  
Michael S. Pickett  
Special Agent  
United States Secret Service

Subscribed and sworn to before me on February 24, 2011

  
CHIEF UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

**PREMISES TO BE SEARCHED**

Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601

2.0 terabyte Western Digital hard drive, serial number WMAZA1626675

HP USB drive, marked 0045SMKBT1 85102

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:
  - A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:
    1. JSTOR
    2. Massachusetts Institute of Technology
    3. Jstor.org
    4. Mit.edu
    5. IP addresses in the class A domain 18.
  - B. Records and tangible objects pertaining to the following topics:
    1. JSTOR
    2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
    3. Records and data stored on JSTOR
    4. Records and data originating on JSTOR
    5. Means of access to JSTOR
    6. Computer software capable of making repeated requests for data and records from JSTOR
    7. Computer software capable of making repeated downloads of records and data from JSTOR



8. MIT's computer network
  9. MIT's physical plant
  10. Remote electronic storage locations
  11. MAC addresses
- C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
- D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;
- E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and
- F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
  2. evidence of computer software that would allow remote access and control of the computer equipment
  3. evidence of the attachment of other computer hardware or storage

media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
5. evidence of the times the computer equipment was used;
6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

- II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

#### DEFINITIONS

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

**Attachment A**

**HP USB drive, marked 0045SMKBT1 85102**

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 1030(a)(2) (intentionally accessing a computer without authorization and obtaining information with a value that exceeds \$5,000), 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage without authorization to a protected computer) and 18 U.S.C. § 1343 (wire fraud), including, without limitation:
  - A. Records and tangible objects pertaining to the following entities, websites, computer networks, and IP addresses:
    1. JSTOR
    2. Massachusetts Institute of Technology
    3. Jstor.org
    4. Mitedu
    5. IP addresses in the class A domain 18.
  - B. Records and tangible objects pertaining to the following topics:
    1. JSTOR
    2. Records and data digitized by JSTOR, including, without limitation, journals digitized by JSTOR
    3. Records and data stored on JSTOR
    4. Records and data originating on JSTOR
    5. Means of access to JSTOR
    6. Computer software capable of making repeated requests for data and records from JSTOR
    7. Computer software capable of making repeated downloads of records and data from JSTOR

8. MIT's computer network
  9. MIT's physical plant
  10. Remote electronic storage locations
  11. MAC addresses
- C. Records and tangible objects pertaining to the existence and identity of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above;
- D. Records and tangible objects pertaining to communications to any third parties in anticipation, during or following the crimes listed above about those crimes;
- E. Records and tangible objects relating to the ownership, occupancy, or use of 950 Massachusetts Avenue, Apartment 320, Cambridge, Massachusetts 02139 and assigned storage locker "C4", Acer Aspire One laptop computer, serial number LUSAX0D001001100E1601, 2.0 terabyte Western Digital hard drive, serial number WMAZA1626675, and HP USB drive, marked 0045SMKBT1 85102; and
- F. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
  2. evidence of computer software that would allow remote access and control of the computer equipment
  3. evidence of the attachment of other computer hardware or storage

media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
5. evidence of the times the computer equipment was used;
6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and
7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

- II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

#### DEFINITIONS

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.



## 13.0 Information Policies

### 13.2 Policy on the Use of Information Technology

Information technology policies ensure that everyone's use of the Institute's computing and telecommunications resources supports its educational, research, and administrative mission in the best possible way. Effective support of the Institute's mission requires complying with relevant legal, contractual, professional, and policy obligations whenever information technology is used. Effective support also means that individuals should not interfere with the appropriate uses of information technology by others.

This policy statement covers privacy of Institute records; information security and preservation; responsible use of MIT computers, networks, and telephones; privacy of electronic communications; and the acquisition and use of third-party products and services.

#### 13.2.1 Privacy of Institute Records

All members of the MIT community are responsible for ensuring that their handling of information about individuals is consistent with the Institute's policy on privacy of information (see Section 11.2). This policy applies to all records of the Institute and to any other appearances of all or part of the information in those records.

The privacy of individuals must be protected, regardless of the form or the location in which the information about them is stored, including computer media. Access to personal information must be limited to authorized users for approved purposes. Such information must be safeguarded from unauthorized access. Individuals who are authorized to access personal information about others should not make unauthorized disclosure or use of it.

The availability of computerized information about individuals may appear to encourage the use of those records for purposes beyond those for which the information was originally collected. Such secondary uses of information about individuals are inappropriate, unless undertaken in accordance with the Institute's policy on privacy.

#### 13.2.2 Information Security and Preservation

MIT has an obligation to provide accurate, reliable information to authorized recipients and to preserve vital records (see Section 13.3 Archival Policy). MIT is increasingly dependent on the accuracy, availability, and accessibility of information stored electronically and on the computing and networking resources that store, process, and transmit this information. Records created and maintained in electronic form are included in the Institute's definition of archival materials.

Individuals who manage or use the information and computing resources required by the Institute to carry out its mission must protect them from unauthorized modification, disclosure, and destruction. Information — including data and software — is to be protected, regardless of the form or medium that carries the information. Protection shall be commensurate with the risk of exposure and with the value of the information and of the computing resources.

#### 13.2.3 Responsible Use of MIT Computers, Networks, and Telephones

MIT's computers, networks, and telephones offer many opportunities to share information on campus and

Case 1:11-cr-10260-NMG Document 81-22 Filed 11/16/12 Page 2 of 3  
to access resources off campus. All members of the MIT community are obligated to use these facilities in accordance with applicable laws, with Institute standards of honesty and personal conduct, and in ways that are responsible, ethical, and professional.

The use of MIT's telephones is restricted to Institute business and necessary personal telephone calls. Necessary personal telephone calls include calls to arrange family and personal schedules, medical-related calls, and other reasonable calls; these calls should be brief. No reimbursement to MIT is required for such calls.

Telephone calls related to personal businesses and activities are prohibited unless a personal telephone credit card is used or an explicit agreement for reimbursement to MIT has been established with the appropriate organization.

MIT's computing and networking facilities and services are to be used for Institute purposes only and not for the benefit of private individuals or other organizations without authorization. Unauthorized access to and use of MIT computer and network services violates this policy.

Members of the Institute community should not take unauthorized actions to interfere with or alter the integrity of MIT computers, networks, telephones, or the information accessed through them. Efforts to restrict or deny access by legitimate users of the Institute's computers, networks, and telephones are unacceptable. Individuals should not use MIT facilities to interfere with or alter the integrity of any other computers, networks, telephones, or information, irrespective of their location.

Destruction, alteration, or disclosure of data or programs belonging to others without authorization is inappropriate. Individuals should not connect unauthorized equipment to or tamper with MIT information technology facilities or equipment. Using any of the information technology resources of the Institute for unethical purposes, such as harassment, is unacceptable.

#### 13.2.4 Privacy of Electronic Communications

Federal laws protect the privacy of users of wire and electronic communications from illegal interception. Individuals who access electronic files or intercept network communications at MIT or elsewhere without appropriate authorization violate Institute policy and may be subject to criminal penalties.

The law also regulates disclosure of information within an electronic mail system by providers of electronic mail services. MIT departments and other providers of electronic mail services at the Institute who are asked to disclose information from an individual's electronic files without the individual's authorization should seek guidance from the Office of the Vice President for Information Systems.

#### 13.2.5 Acquisition and Use of Third-Party Products and Services

Special restrictions are often placed on the use of information technology products and services — such as hardware, software, documentation, and databases — acquired from outside sources. Members of the MIT community are required to abide by the restrictions imposed by suppliers on information technology products and services acquired for use at the Institute.

Unless it has been placed in the public domain, most third-party software is protected by copyright law. Under US copyright law, it is illegal to duplicate copyrighted software or documentation — except for one archival copy — without the permission of the copyright owner. Unauthorized copying includes lending software to others so that they can make unauthorized copies, as well as letting someone use your computer to make an unauthorized copy. It is illegal to distribute unauthorized copies of software by any means, including a computer network.

Use of hardware, software, databases, and documentation may be further restricted by patent law, as a trade secret, or by contract law in the form of a license or other agreement. When a department, laboratory, center, or individual acquires hardware, software, documentation, or access to proprietary databases from outside sources for use at MIT, the department is responsible for obtaining Institute approval that the terms and conditions of any associated license or other agreement are consistent with relevant Institute policy, such as the research policy statements and the policies on Intellectual Property (see Section 13.1).

When supervisors, instructors, or others arrange for authorized distribution of information technology products and services from outside sources, those individuals are responsible for ensuring that the people having access to the products and services are advised of all the associated usage restrictions.

CLOSED, PROSE-NP, TYPE-F

**U.S. District Court  
District of Columbia (Washington, DC)  
CIVIL DOCKET FOR CASE #: 1:11-cv-01463-UNA**

STEPNEY v. JSTOR et al  
Assigned to: Unassigned  
Demand: \$5,000,000,000  
Cause: 42:1983 Civil Rights Act

Date Filed: 08/12/2011  
Date Terminated: 08/12/2011  
Jury Demand: None  
Nature of Suit: 890 Other Statutory Actions  
Jurisdiction: Federal Question

**Plaintiff****JO ANN MYERS STEPNEY**

represented by **JO ANN MYERS STEPNEY**  
781 Embarcadero Del Norte #5  
Goleta, CA 93117  
(805) 685-4304  
PRO SE

V.

**Defendant****JSTOR****Defendant****ANDREW W. MELLON FOUNDATION****Defendant****ITHAKA**

Date Filed	#	Docket Text
08/12/2011	1	COMPLAINT against ANDREW W. MELLON FOUNDATION, ITHAKA, JSTOR filed by JO ANN MYERS STEPNEY. (Attachments: # 1 Civil Cover Sheet)(md, ) (Entered: 08/12/2011)
08/12/2011		SUMMONS Not Issued as to ANDREW W. MELLON FOUNDATION, ITHAKA, JSTOR. (md, ) (Entered: 08/12/2011)
08/12/2011	2	MOTION for Leave to Proceed in forma pauperis by JO ANN MYERS STEPNEY. (md, ) (Entered: 08/15/2011)
08/12/2011	3	MEMORANDUM AND OPINION. Signed by Judge Henry H. Kennedy on 08/02/2011. (md, ) (Entered: 08/15/2011)
08/12/2011	4	ORDER DISMISSING PRO SE CASE WITH PREJUDICE. Ordered that the application of the plaintiff to proceed in forma pauperis is GRANTED. This is a final appealable Order. SO ORDERED.. Signed by Judge Henry H. Kennedy on 08/02/2011. (md, ) (Entered: 08/15/2011)

<b>PACER Service Center</b>			
<b>Transaction Receipt</b>			
11/30/2011 10:12:58			
<b>PACER Login:</b>	us8542	<b>Client Code:</b>	
<b>Description:</b>	Docket Report	<b>Search Criteria:</b>	1:11-cv-01463-UNA
<b>Billable Pages:</b>	1	<b>Cost:</b>	0.08

**RIF**

265

## **FARON PARAMORE (GPA)**

---

**From:** (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) @mail.house.gov  
**Sent:** Friday, February 01, 2013 10:57 AM  
**To:** FARON PARAMORE (GPA)  
**Subject:** RE: U.S. Secret Service - Swartz briefing today.

2157 Rayburn. Yes, I'm the contact now that (b)(6) is out. A bunch of my guys are out, so I'm covering a lot. Give a call if you need anything in advance. (b)(6),(b)(7)(C)

-----Original Message-----

**From:** FARON PARAMORE (GPA) [mailto:(b)(6),(b)(7)(C)@uss.s.dhs.gov]  
**Sent:** Friday, February 01, 2013 10:53 AM  
**To:** (b)(6),(b)(7)(C)  
**Subject:** U.S. Secret Service - Swartz briefing today.  
**Importance:** High

Good Morning (b)(6), hope you are well.

(b)(6),(b)(7)(C) I just received an email from (b)(6), informing me that he was out of the office today and that you would be our POC for the briefing this afternoon at 1pm.

Sir, can you please advise where we should meet you for the briefing at 1pm.

Thanks much.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

**Ph:** (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
(b)(6),(b)(7)(C) Cell  
(202) 406-5740 Fax

-----Original Message-----

**From:** FARON PARAMORE (GPA)  
**Sent:** Friday, February 01, 2013 10:28 AM  
**To:** (b)(6),(b)(7)(C)  
**Cc:** FARON PARAMORE (GPA)  
**Subject:** U.S. Secret Service - Swartz briefing today.  
**Importance:** High

Good Morning (b)(6),(b)(7)(C) hope you are well.

Just left you a voice mail.

(b)(6),(b)(7)(C) couple of things.

1) Can I please get the building and room # of where the briefing will be held today.

2) When you have a chance, can you please give me a call OR let me know what is a good time to contact you concerning the 6E issue.

Our Chief Counsel's office has (b)(5)

(b)(5)

It is my understanding that DOJ will not be participating with the briefing this afternoon. That their briefing may take place at a later tbd time.

Respectfully, we (USSS) will provide information on our investigation. We will not speak to matters that fall under DOJ's purview.

Again, I think you will be pleased with the information we will provide.

Thanks much.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

## **FARON PARAMORE (GPA)**

---

**From:** (b)(6),(b)(7)(C) [redacted]@mail.house.gov]  
**Sent:** Monday, January 28, 2013 9:25 AM  
**To:** FARON PARAMORE (GPA)  
**Cc:** (b)(6),(b)(7)(C) [redacted]  
**Subject:** RE: Briefing

Hi Faron,

Thanks for the message. Hope you had a nice weekend as well.

As for the 6E concerns, public reports indicate that the charges were dropped (see below from the *L.A. Times*).

We look forward to seeing you on Friday.

Thanks,

(b)(6),(b)(7)(C) [redacted]

## **Feds drop charges against late Internet activist Aaron Swartz**

Federal prosecutors in Boston have dropped charges against Internet activist Aaron Swartz after his death.  
(Michael Francis McElroy / New York Times via Associated Press / January 30, 2009)  
By Jessica Guynn

January 14, 2013, 10:38 a.m.

Federal prosecutors in Boston have dropped charges against Internet activist Aaron Swartz.

Swartz, 26, was found dead Friday in his New York apartment. He apparently had hanged himself.

Prosecutors filed the notice of dismissal on Monday.

Swartz's family blamed his death on "prosecutorial overreach."

The U.S. attorney's office could not be reached for comment.

Federal prosecutors alleged Swartz used MIT's computers to illegally access millions of academic articles through the JSTOR database, a subscription service for scholarly articles. He was indicted in 2011 and was scheduled to go to trial on 13 counts including computer fraud. Swartz faced the possibility of millions of dollars in fines and up to 35 years in prison.

The case was seen as a showdown pitting the government and commercial interests against Internet "freedom fighters."



MIT President L. Rafael Reif on Sunday appointed Hal Abelson, a professor of computer science and engineering and a founding director of Creative Commons and the Free Software Foundation, to "lead a thorough analysis of MIT's involvement."

As news spread over the weekend of Swartz's death, the Web collectively mourned for a brilliant young technologist and activist who wanted to set the world's information free yet could never escape his own demons.

Confided one friend: "I'm not surprised that this is how his life ended, and I bet many others feel the same way. So sad, he had so much potential and not enough joy in his life."

Swartz was just 14 when he helped create RSS, a tool that distributes online content. He was one of the founders of the social news site Reddit, which was bought by Conde Nast. But he was best known as an activist for free and open access to the world's information.

"Everything he did was aimed at world-changing and at activism," said friend and historian Rick Perlstein.

Now his death is being used to question government's aggressive criminal prosecution of Internet activists.

Anonymous allegedly hacked MIT's website and left a tribute for Swartz: "We do not consign blame or responsibility upon MIT for what has happened, but call for all those feel heavy-hearted in their proximity to this awful loss to acknowledge instead the responsibility they have — that we all have — to build and safeguard a future that would make Aaron proud."

---

From: FARON PARAMORE (GPA) [mailto:(b)(6),(b)(7)(C)]<(b)(6),(b)(7)(C)@uss.s.dhs.gov>  
Sent: Friday, January 25, 2013 3:47 PM  
To: (b)(6),(b)(7)(C)  
Cc: (b)(6),(b)(7)(C)  
Subject: RE: Briefing

Good afternoon (b)(6),(b)(7)(C) hope you are well.

Friday, February 1, 2013 at 1pm should work well for us.

(b)(6),(b)(7)(C) we have absolutely no problem coming up to provide the briefing.

Our Boston Office is touching base with the US Attorney's Office up there, to see where we are with any 6E Grand Jury materials. If they dismiss / drop the charges then I think it would make the 6E issue "go away" and it would not be a concern at all.

Thanks much, hope you have a pleasant weekend.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
(b)(6),(b)(7)(C) Cell  
(202) 406-5740 Fax

**From:** (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@mail.house.gov]  
**Sent:** Friday, January 25, 2013 1:58 PM  
**To:** FARON PARAMORE (GPA)  
**Cc:** (b)(6),(b)(7)(C)  
**Subject:** RE: Briefing

Hi Faron,

Thanks for your voicemail.

We would like to schedule the briefing for 2/1/2013 at 1:00 p.m. at our offices. We will provide further information about the specific room.

Please let me know if that works.

Sincerely,

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

**From:** FARON PARAMORE (GPA) [mailto:(b)(6),(b)(7)(C)@usss.dhs.gov]  
**Sent:** Thursday, January 17, 2013 12:11 PM  
**To:** (b)(6),(b)(7)(C)  
**Cc:** (C)  
**Subject:** RE: Briefing

Good afternoon (b)(6),(b) hope you are well.

Thanks for the email.

Sure thing, be back in touch soon.

Thanks.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

**From:** (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@mail.house.gov]  
**Sent:** Thursday, January 17, 2013 11:54 AM  
**To:** FARON PARAMORE (GPA)  
**Cc:** (b)(6),(b)(7)(C)  
**Subject:** Briefing

Hi Faron,

Thanks for speaking with us about the briefing. Please let us know when you have further information.

Sincerely,

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

**U.S. House of Representatives**  
**Committee on Oversight and Government Reform**  
**Darrell Issa, Chairman**

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

**All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.**

## **FARON PARAMORE (GPA)**

**From:** (b)(6),(b)(7)(C) (OLA) (b)(6),(b)(7)(C)@usdoj.gov  
**Sent:** Tuesday, January 22, 2013 11:04 AM  
**To:** FARON PARAMORE (GPA)  
**Cc:** (b)(6),(b)(7)(C)@hq.dhs.gov  
**Subject:** RE: U.S. Secret Service - Aaron Swartz case out of Boston

DAD Paramore:

Consult with outside agency.

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

Attorney Advisor  
U.S. DEPARTMENT OF JUSTICE  
Office of Legislative Affairs

(b)(6),(b)(7)(C)@sdoj.gov

(b)(6),(b)(7)(C) - direct

-----Original Message-----

**From:** FARON PARAMORE (GPA) [mailto:(b)(6),(b)(7)(C)@uss.s.dhs.gov]  
**Sent:** Tuesday, January 22, 2013 10:59 AM  
**To:** (b)(6),(b)(7)(C) (OLA)  
**Cc:** (b)(6),(b)(7)(C)@hq.dhs.gov  
**Subject:** U.S. Secret Service - Aaron Swartz case out of Boston

Good Morning Ms. (b)(6), hope you are well.

Ma'am, my name is Faron K. Paramore. I serve as the Deputy Assistant Director in the Office of Congressional Affairs for the U.S. Secret Service.

Last Thursday afternoon (1/17/13) I was contacted by a Mr. (b)(6),(b)(7)(C) professional staff with the House Oversight & Government Reform Committee (Majority Staff - Chairman Issa), requesting to receive a briefing from the U.S. Secret Service regarding our role / investigation of the Aaron Swartz case out of Boston, MA.

Ma'am, at your convenience would it be possible for me to give you a call to discuss this matter.

Thank you very much for your time.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

Note the Issa comments towards the end of the article <http://thehill.com/blogs/hillicon-valley/technology/277709-justice-department-defends-prosecution-of-activist-swartz>

\* Previous TJX hacking case - Same prosecutor and the suspect also committed suicide:

<http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html>

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

## **FARON PARAMORE (GPA)**

**From:** (b)(6),(b)(7)(C) [redacted] HQ.DHS.GOV]  
**Sent:** Tuesday, January 22, 2013 11:03 AM  
**To:** FARON PARAMORE (GPA)  
**Subject:** RE: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

checking

**From:** FARON PARAMORE (GPA) [mailto:(b)(6),(b)(7)(C)@usss.dhs.gov]  
**Sent:** Tuesday, January 22, 2013 10:53 AM  
**To:** (b)(6),(b)(7)(C) [redacted]  
**Cc:** WILLIAMS LYNDA R  
**Subject:** RE: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

(b)(6),(b)(7)(C) Does DHS OLA have any concerns with us providing us a briefing to the OGR STAFF on this issue?

NOTE: We (USSS) will ONLY talk about our role in investigating this case. We will NOT speak to any aspect of "Plea Agreements" etc.

Thx. Faron

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) [redacted] Direct line  
Cell  
(202) 406-5740 Fax

**From:** (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@HQ.DHS.GOV]  
**Sent:** Tuesday, January 22, 2013 10:41 AM  
**To:** FARON PARAMORE (GPA)  
**Subject:** RE: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Hi Faron --

I hope you are resting from the wonderful and what seemed to be a well coordinated inauguration. I apologized, I told you Friday I would send you my POCs for DoJ Congressional (below). (b)(6) is an atty and works in all areas of DoJ where I believe (b)(6) may specialize in illicit drugs but both should be able to point you in the right direction.

(b)(6),(b)(7)(C) [redacted]@usdoj.gov  
(b)(6),(b)(7)(C) [redacted]@usdoj.gov

**From:** FARON PARAMORE (GPA) [mailto:(b)(6),(b)(7)(C)@usss.dhs.gov]  
**Sent:** Friday, January 18, 2013 3:40 PM  
**To:** (b)(6),(b)(7)(C) [redacted]  
**Cc:** PARAMORE FARON K  
**Subject:** From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Good afternoon (b)(6),(b)(7)(C) hope you are well.

(b)(6),(b)(7)(C) just left you a v/m.

Over the last year and a half our Boston Field Office / New England Electronics Crimes Task Force was working a cyber case. Our Suspect was a Mr. Aaron Swartz's. Long story short - Swartz killed himself about a week ago. His federal trial was suppose to start in a month or so.

NOW, there have been numerous articles on the web about how the "Federal Gov't" was heavy handed in this case.

Late yesterday afternoon I received a call from Chairman Issa's staff requesting to receive a briefing possible next week.

Want to make sure DHS is in the loop on what actually happened.

Also, we will need to coordinate with DOJ Congressional Affairs on this. The USSS will ONLY speak to our role in this case. DOJ (The U.S. Attorneys Office has a big part in this also).

Please give me a call when you have a moment so I can brief you.

See links below.

Thanks. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
(b)(6),(b)(7)(C) Cell  
(202) 406-5740 Fax

---

From: (b)(6),(b)(7)(C) (GPA)  
Sent: Thursday, January 17, 2013 1:46 PM  
To: FARON PARAMORE (GPA)  
Cc: LYNDIA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA)  
Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Faron,

Here are some -- see attached.

Also - Here are a couple more things that (b)(6),(b)(7)(C) found:

- Note the Issa comments towards the end of the article  
<http://thehill.com/blogs/hillicon-valley/technology/277709-justice-department-defends-prosecution-of-activist-swartz>
- Previous TJX hacking case - Same prosecutor and the suspect also committed suicide:  
<http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html>

Let us know what else you need.

Thanks,

(b)(6),(b)(7)(X)

-----Original Message-----

From: (b)(6),(b)(7)(C) (GPA)

Sent: Thursday, January 17, 2013 1:39 PM

To: (b)(6),(b)(7)(C) (GPA)

Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

<http://crooksandliars.com/karoli/unanswered-question-why-was-secret-service->

<http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html>

-----Original Message-----

From: FARON PARAMORE (GPA)

Sent: Thursday, January 17, 2013 1:35 PM

To: (b)(6),(b)(7)(C) (GPA)

Cc: LYNDIA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA)

Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

(b)(6),(b)(7)(X) can you pull down any / all articles you can find on the internet concerning this guy

Mr. Aaron Swartz.

Issa's office just called and are looking for a briefing tbd time next week.

Thx. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

-----Original Message-----

From: EDWIN DONOVAN (GPA)

Sent: Thursday, January 17, 2013 12:54 PM

To: HUGH DUNLEAVY (INV); JANE MURPHY (INV); PAUL MORRISSEY (GPA); LEE FIELDS (INV); JONATHAN BARTLETT (CID)

Cc: (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); FARON PARAMORE (GPA); (b)(6),(b)(7)(C) (GPA); LYNDIA WILLIAMS (GPA)

Subject: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Attached is an article from Time.com discussing Aaron Swartz's suicide and reaction from some members of Congress.



Link to article: <http://business.time.com/2013/01/16/aaron-swartzs-suicide-triggers-response-from-us-lawmakers/>

**All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.**



## **FARON PARAMORE (GPA)**

**From:** (b)(6),(b)(7)(C) [redacted] HQ.DHS.GOV  
**Sent:** Tuesday, January 22, 2013 10:41 AM  
**To:** FARON PARAMORE (GPA)  
**Subject:** RE: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Hi Faron --

I hope you are resting from the wonderful and what seemed to be a well coordinated inauguration. I apologized, I told you Friday I would send you my POCs for DoJ Congressional (below). (b)(6) is an atty and works in all areas of DoJ where I believe (b)(6) may specialize in illicit drugs but both should be able to point you in the right direction.

(b)(6),(b)(7) [redacted] usdoj.gov

(b)(6),(b)(7)(C) [redacted] usdoj.gov

---

**From:** FARON PARAMORE (GPA) [mailto:(b)(6),(b)(7)(C) [redacted] usss.dhs.gov]  
**Sent:** Friday, January 18, 2013 3:40 PM  
**To:** (b)(6),(b)(7)(C) [redacted]  
**Cc:** PARAMORE FARON K  
**Subject:** From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Good afternoon (b)(6),(C) [redacted] hope you are well.

(b)(6) [redacted] just left you a v/m.

Over the last year and a half our Boston Field Office / New England Electronics Crimes Task Force was working a cyber case. Our Suspect was a Mr. Aaron Swartz's. Long story short - Swartz killed himself about a week ago. His federal trial was suppose to start in a month or so.

NOW, there have been numerous articles on the web about how the "Federal Gov't" was heavy handed in this case.

Late yesterday afternoon I received a call from Chairman Issa's staff requesting to receive a briefing possible next week.

Want to make sure DHS is in the loop on what actually happened.

Also, we will need to coordinate with DOJ Congressional Affairs on this. The USSS will ONLY speak to our role in this case. DOJ (The U.S. Attorneys Office has a big part in this also).

Please give me a call when you have a moment so I can brief you.

See links below.

Thanks. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line

(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

From: (b)(6),(b)(7)(C) (GPA)  
Sent: Thursday, January 17, 2013 1:46 PM  
To: FARON PARAMORE (GPA)  
Cc: LYNDIA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA)  
Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Faron,

Here are some -- see attached.

Also - Here are a couple more things that (b)(6),(b)(7)(C) found:

- Note the Issa comments towards the end of the article  
<http://thehill.com/blogs/hillicon-valley/technology/277709-justice-department-defends-prosecution-of-activist-swartz>
- Previous TJX hacking case - Same prosecutor and the suspect also committed suicide:  
<http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html>

Let us know what else you need.

Thanks.

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

-----Original Message-----

From: (b)(6),(b)(7)(C) (GPA)  
Sent: Thursday, January 17, 2013 1:39 PM  
To: (b)(6),(b)(7)(C) (GPA)  
Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

<http://crooksandliars.com/karoli/unanswered-question-why-was-secret-service->

<http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html>

-----Original Message-----

From: FARON PARAMORE (GPA)  
Sent: Thursday, January 17, 2013 1:35 PM  
To: (b)(6),(b)(7)(C) (GPA)  
Cc: LYNDIA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA)  
Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

(b)(6),(b)(7)(C) can you pull down any / all articles you can find on the internet concerning this guy

Mr. Aaron Swartz.

Issa's office just called and are looking for a briefing tbd time next week.

Thx. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
(b)(6),(b)(7)(C) Cell  
(202) 406-5740 Fax

-----Original Message-----

From: EDWIN DONOVAN (GPA)  
Sent: Thursday, January 17, 2013 12:54 PM  
To: HUGH DUNLEAVY (INV); JANE MURPHY (INV); PAUL MORRISSEY (GPA); LEE FIELDS (INV); JONATHAN BARTLETT (CID)  
Cc: (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); FARON PARAMORE (GPA); (b)(6),(b)(7)(C) (GPA); LYNDIA WILLIAMS (GPA)  
Subject: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Attached is an article from Time.com discussing Aaron Swartz's suicide and reaction from some members of Congress.

Link to article: <http://business.time.com/2013/01/16/aaron-swartzs-suicide-triggers-response-from-us-lawmakers/>

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

## **FARON PARAMORE (GPA)**

---

**From:** FREDERICK SELLERS (INV)  
**Sent:** Thursday, January 17, 2013 2:12 PM  
**To:** FARON PARAMORE (GPA)  
**Subject:** Re: Articles regarding Aaron Swartz

Thanks.

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Thursday, January 17, 2013 02:11 PM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV); FREDERICK SELLERS (INV)  
**Cc:** (b)(6),(b)(7)(C) (GPA); EDWIN DONOVAN (GPA); PAUL MORRISSEY (GPA)  
**Subject:** Articles regarding Aaron Swartz

Just fyi.

Quotes from several Hill folks in the HILL clip below.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

---

**From:** (b)(6),(b)(7)(C) (GPA)  
**Sent:** Thursday, January 17, 2013 1:46 PM  
**To:** FARON PARAMORE (GPA)  
**Cc:** LYNDIA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA)  
**Subject:** FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Faron,

Here are some -- see attached.

Also - Here are a couple more things that (b)(6), found:

- Note the Issa comments towards the end of the article  
<http://thehill.com/blogs/hillicon-valley/technology/277709-justice-department-defends-prosecution-of-activist-swartz>
- Previous TJX hacking case - Same prosecutor and the suspect also committed suicide:  
<http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html>

Let us know what else you need.

Thanks,

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

-----Original Message-----

From: (b)(6),(b)(7)(C) (GPA)

Sent: Thursday, January 17, 2013 1:39 PM

To: (b)(6),(b)(7)(C) (GPA)

Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

<http://crooksandliars.com/karoli/unanswered-question-why-was-secret-service->

<http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html>

-----Original Message-----

From: FARON PARAMORE (GPA)

Sent: Thursday, January 17, 2013 1:35 PM

To: (b)(6),(b)(7)(C) (GPA)

Cc: LYNDA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA)

Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

(b)(6),(b)(7) can you pull down any / all articles you can find on the internet concerning this guy

Mr. Aaron Swartz.

Issa's office just called and are looking for a briefing tbd time next week.

Thx. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
(b)(6),(b)(7)(C) Cell  
(202) 406-5740 Fax

-----Original Message-----

From: EDWIN DONOVAN (GPA)

Sent: Thursday, January 17, 2013 12:54 PM

To: HUGH DUNLEAVY (INV); JANE MURPHY (INV); PAUL MORRISSEY (GPA); LEE FIELDS (INV); JONATHAN BARTLETT (CID)

Cc: (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); FARON PARAMORE (GPA); (b)(6),(b)(7)(C) (GPA); LYNDA WILLIAMS (GPA)

Subject: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Attached is an article from Time.com discussing Aaron Swartz's suicide and reaction from some members of Congress.

Link to article: <http://business.time.com/2013/01/16/aaron-swartzs-suicide-triggers-response-from-us-lawmakers/>

**FARON PARAMORE (GPA)**

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Friday, February 01, 2013 10:13 AM  
**To:** (b)(6),(b)(7)(C) @usdoj.gov  
**Cc:** FARON PARAMORE (GPA)  
**Subject:** J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopses  
**Attachments:** Swartz INV Brief 1-29-2013.pdf

**Importance:** High

Sir, here you go.

Thanks much.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

## memorandum

DATE: January 29, 2013  
REPLY TO: SAIC – Boston Field Office  
ATTN OF:  
SUBJECT: Aaron Swartz Investigation  
TO: AD – Office of Investigations

U.S. Secret Service  
775.210  
J-102-775-600710-S

Reference is made to the multiple telephone and electronic mail conversations regarding the above subject case, in particular the January 22, 2013, request by DAD Hugh Dunleavy, Office of Investigations, for additional information regarding the criminal investigation of Aaron Swartz.

Further reference is made to the multiple US Secret Service Investigative Reports in case number J-102-775-600710-S. The below information is being provided as a brief outline in said case as it relates to the criminal investigation. The Department of Justice and the US Attorney's Office, District of Massachusetts, is the appropriate entity to consult in reference to the prosecution and court proceedings in this case.

**Aaron Swartz Investigation Background**

**September 24, 2010**

Late during the night of September 24, 2010, an unidentified individual registered his computer on Massachusetts Institute of Technology's (MIT) campus and obtained a guest account on MIT's computer network. The individual did not provide his true identity at this or any subsequent time, and neither MIT personnel nor law enforcement officers knew the individual's name until his arrest months later. The individual registered his computer by specifying his name as "Gary Host," a pseudonym, and his e-mail address as ghost@mailinator.com, a disposable e-mail address by virtue of its requiring no initial e-mail registration and keeping no records of e-mail access. Before assigning the computer an Internet Protocol (IP) address, MIT's network automatically collected the computer's owner-created name — "ghost laptop" — and the unique identifying number associated with the computer's Internet networking hardware, known as the computer's Media Access Control (MAC) address. These are standard login and communication procedures.

MIT's Dynamic Host Configuration Protocol (DHCP) computer server then used a standard Internet protocol to assign the individual an IP address (18.55.6.215) for use while on the network. The network kept records of the computer's registration information, its IP and its MAC addresses. These records are standard computer-networking records, and did not include any computer commands that the individual typed in or ran, or any data that the computer downloaded.

**September 25, 2010**



The day after registering the "ghost laptop," the unidentified individual used the "ghost laptop" to systematically access and rapidly download an extraordinary volume of articles from JSTOR (short for Journal Storage, is a digital library founded in 1995. Originally containing digitized back issues of academic journals, it now also includes books and primary sources, and current issues of journals) by using a software program that sidestepped JSTOR's computerized limits on the volume of each user's downloads. The downloads and requests for downloads were so numerous, rapid, and massive that they impaired the performance of JSTOR's computers.

As JSTOR, and then MIT, became aware of these downloads and problems, both attempted to block the individual's computer from further communications. On the evening of September 25, 2010, after suffering hundreds of thousands of downloads from the ghost laptop, JSTOR temporarily ended the downloads by blocking network access from the computer at IP address 18.55.6.215.

The next day, however, the ghost laptop's user obtained a new IP address from MIT's network, changing the last digit in its IP address by one digit from 18.55.6.215 to 18.55.6.216. This defeated JSTOR's IP address block, enabling the ghost laptop to resume furiously downloading articles from JSTOR. This downloading continued until the middle of September 26, when JSTOR identified it and blocked communication from IP address 18.55.6.216 as well. The September 25 and 26 downloads had impaired JSTOR's computers and misappropriated significant portions of its archive. Because the download requests had originated from two MIT IP addresses that had begun with 18.55.6 — that is, 18.55.6.215 and 18.55.6.216 — JSTOR began blocking a broader range of MIT IP addresses on September 26. The new block prevented MIT researchers assigned MIT IP addresses 18.55.6.0 through 18.55.6.255 (as many as 253 computers) from performing research through JSTOR's archive for three to four days.

#### September 27, 2010

When JSTOR notified MIT of the continuing problems; MIT banned the "ghost laptop" from using its network as well. To do this, MIT terminated the ghost laptop's guest registration and prohibited the computer, as identified by its hardware MAC address, from being assigned a new IP address again through the guest registration process.

#### October 2, 2010

Less than a week after JSTOR and MIT had barred the ghost laptop from communicating with their networks, the unidentified individual obtained yet another guest connection for the ghost laptop on MIT's network. Having recognized that MIT or JSTOR had blocked his ghost laptop by recognizing its MAC address, the individual now manipulated the ghost laptop's MAC address to mislead MIT into believing that he was a new and different guest registrant.

#### October 8, 2010

The unidentified individual connected a second computer to MIT's network and created another guest account using pseudonyms similar to those he had used with the "ghost laptop". He registered the new computer under the name "Grace Host", a temporary email address of

ghost42@mailinator.com, and a computer client name of "ghost macbook."

#### October 9, 2010

The unknown individual activated the ghost laptop and the ghost macbook to download JSTOR's articles once again. The downloads came so fast and numerous that the individual again significantly impaired the operation of some of JSTOR's computers.

Once again, MIT could not identify who was controlling these computers or where they were physically located, and JSTOR could not isolate the interloper to a consistent IP address that could be blocked. Consequently, JSTOR blocked access by and to every computer using an MIT IP address campus-wide for approximately three days, again depriving legitimate MIT users from accessing JSTOR's services. MIT blocked computers using the ghost laptop's and the ghost macbook's MAC addresses as well.

Nevertheless, between the end of October and January 6, 2011, the unidentified hacker obtained at least three new IP addresses and assigned his computer two new MAC addresses. He also moderated the speed of the downloads, which made them less noticeable to JSTOR. The exfiltration of JSTOR's collection was nonetheless extreme. During this period, the individual downloaded well over a million of JSTOR's articles.

Because the hacker had modified the speed of his downloads, JSTOR did not notice his latest downloads until around December 25, 2010. Once detected, however, JSTOR provided MIT with the hacker's latest IP address. Now that MIT's network security personnel had a more robust set of network tools, they could consult network traffic routing records and trace the IP address back to a concrete physical location on campus.

#### January 4, 2011

An MIT network security analyst traced the hacker's IP address to a network switch located in a basement wiring closet in MIT's Building 16. Building 16's street level doors have no-trespassing signs posted on them. The wiring closet is protected by a pair of locked steel doors. The closet is generally locked, but at that time its lock could be forced by a quick jerk of its double doors. When MIT personnel entered the closet, they found a cardboard box with a wire leading from it to a computer network switch.

Hidden under the box was the ghost laptop, an Acer-brand laptop, connected to a separate hard drive for excess storage. The network cable connected the laptop to the network switch, thus giving the laptop Internet access. The laptop's direct connection to the network switch was unusual because MIT does not connect computers directly to those switches.

### **LAW ENFORCEMENT IS NOTIFIED**

#### January 4, 2011

MIT personnel called the MIT Police to the scene, who, in turn, called a USSS New England Electronic Crimes fulltime Task Force Officer (TFO) directly. The TFO is a Detective from Cambridge Police. Three members of the task force respond to the scene, a USSS Special

Agent, a Boston Police Detective who is a fulltime TFO and the Cambridge Police TFO who received the call. A Cambridge Police Crime Scene Unit was summoned to the scene for processing. Over the course of the morning and early afternoon of January 4th, MIT and law enforcement officers collaboratively took several steps to identify the perpetrator and learn what he was up to:

- (1) Cambridge Police crime scene specialists fingerprinted the laptop's interior and exterior and the external hard drive and its enclosure;
- (2) MIT placed and operated a video camera inside the closet, which, as discussed below, later recorded the hacker (subsequently identified as Aaron Swartz) entering the wiring closet and performing tasks within it;
- (3) The Secret Service opened the laptop and sought to make a copy of its volatile memory aka Random Access Memory (RAM), which would automatically be destroyed when the laptop's power was turned off, but the effort resulted in their seeing only the laptop's user sign-in screen;
- (4) MIT connected a second laptop to the network switch in order to record the laptop's communications, a type of recording often referred to as a "packet capture;" (b)(3) Rule 6E

(b)(3) Rule 6E

- (5) Beginning on January 4, 2011, MIT agreed to provide, and later provided, the Secret Service copies of network logs pertaining to the ghost laptop and ghost macbook between September 24, 2010 and January 6, 2011, some of which records were provided consensually, the remainder of which were provided pursuant to a subpoena.

By mid-day on January 4th, MIT and law enforcement personnel had completed their initial crime scene investigation. Experience led them to believe that merely removing the hacker's computer equipment would more than likely result in his renewing his efforts elsewhere. So, rather than take the hacker's equipment away, MIT and law enforcement instead restored the closet to its initial appearance upon discovery, and monitored who entered the closet and handled the laptop. MIT installed an IP camera in the closet to accomplish the monitoring. In this way, the hacker would not necessarily know that his criminal tools had been discovered, his identity might be uncovered, and he could be stopped.

Within an hour of their departure, the unidentified hacker returned. After entering the wiring closet and shutting the doors behind him, the hacker replaced the hard drive connected to the laptop with a new one he took from his backpack, and then concealed his equipment once again underneath the cardboard box. This activity was captured by the video camera that was installed inside the wiring closet.

**Agents made notification to the US Attorney's Office, District of Massachusetts, regarding the facts of the investigation.**

### January 6, 2011

The unknown subject hacker returned to the wiring closet yet again. This time, worried about being identified, the hacker covered his face with his bicycle helmet as he entered the closet. Once inside and with the door closed, the hacker disconnected the laptop and placed it, the external hard drive, and the network cable in his backpack. As he left, he again hid his face with his bicycle helmet. This activity was also captured by the camera installed within the wiring closet. By January 6, 2011, the hacker had downloaded a major portion of the six to seven million articles then contained in JSTOR's digitized database.

Shortly after 2:00pm on January 6, 2011, MIT Police (b)(6), (b)(6),(b)(7)(C) who had been involved in the investigation, was heading down Massachusetts Avenue within a mile of MIT when he spotted a bicyclist who looked like the hacker caught on the wiring closet video. (b)(6),(b)(7)(C) identified himself as a police officer. After a brief exchange, the individual dropped his bike to the ground and ran away. The individual was chased, apprehended, arrested, and subsequently identified as Aaron Swartz. During a search incident to arrest, Cambridge police found a USB storage drive in Swartz's backpack, which they seized and stored as evidence.

Approximately an hour later, MIT technical staff used computer routing and addressing records to locate Swartz's ghost laptop and hard drive in the Student Information Processing Board's office in MIT's student center. Law enforcement found the equipment on the floor under a desk connecting it to the MIT network. The equipment was subsequently seized and stored as evidence by Cambridge Police. Aaron Swartz was charged by the Commonwealth in a criminal complaint alleging Breaking and Entering into MIT's property with intent to commit a felony, and was subsequently indicted by a Massachusetts grand jury for the same charge along with the theft of JSTOR's electronically processed or stored data, and accessing a computer system without authorization.

### February 9, 2011

The Secret Service applied for and subsequently obtained a federal search warrant for Aaron Swartz's apartment, located at 950 Massachusetts Avenue in Cambridge.

### February 11, 2011

Agents and a Task Force Officer executed the federal search warrant on Swartz's residence.

Immediately after the search of the residence was completed a second federal search warrant was applied for and issued for Swartz's worksite. That search warrant was executed on Swartz's work address, 124 Mount Auburn Street in Cambridge, The Safra Center for Ethics at Harvard Law School.

### February 24, 2011

The Secret Service obtained a federal search warrant to seize and search the laptop, the hard drive in the enclosure and the USB storage device that was being secured within the Cambridge Police Evidence Unit.

**February 25, 2011**

The evidence is transferred from the Cambridge Police to the USSS Boston Field Office pursuant to the search warrant.

**May 16, 2011**

Swartz was served in hand, at his residence with a federal seizure and forfeiture warrant for the JSTOR property in his possession. Swartz refused to comply with the federal seizure and forfeiture warrant.

**June 7, 2011**

USSS BFO Agent responded to the Law Offices of Goode and Cormier, 83 Atlantic Ave Boston, MA. Attorney Goode was at the present time, Swartz's defense counsel. At that location USSS took custody of (4) four Hard Disk Drives (HDD) containing 8,989,635 articles (PDF's) that had been downloaded from the JSTOR website through MIT's network by Swartz.

**July 14, 2011**

Federal Grand Jury returns a true bill against Aaron Swartz for Wire Fraud, Computer Fraud and data theft.

**July 19, 2011**

Aaron Swartz is arrested and arraigned at the US District Court, District of Massachusetts in Boston, MA.

Again, the above is being provided as a brief synopsis of the criminal investigation involving Aaron Swartz. Questions concerning the above maybe directed to the case agent, SA [redacted] and TFO [redacted], Boston Field Office, New England Electronic Crimes Task Force.

Steven D. Ricciardi  
Special Agent in Charge

## **FARON PARAMORE (GPA)**

---

**From:** (b)(6),(b)(7)(C) (INV)  
**Sent:** Thursday, January 31, 2013 11:29 AM  
**To:** (b)(6),(b)(7)(C) (LEG)  
**Cc:** dadmw; DONNA CAHILL (LEG); HUGH DUNLEAVY (INV); FARON PARAMORE (GPA)  
**Subject:** J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopsis  
**Attachments:** Swartz INV Brief 1-29-2013.pdf  
  
**Importance:** High

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

Attached for OCC review is the BOS summary of the J-102-775-600710-S investigation.  
This summary was offered to the USAO BOS for review and was declined.

I am scheduled to appear before the House Oversight & Gov't Reform Committee (OGR) Chairman Issa Staff on Friday, February 1, 2013.

SAJC BOS advises that the synopsis contains only information available in the unsealed indictment of Suspect Swartz. Pending your review, GPA will likely push to its DOJ counterpart.

Call w/ questions. V/r Hugh

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Wednesday, January 30, 2013 9:53 AM  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** FREDERICK SELLERS (INV)  
**Subject:** Final Draft of INV Requested Swartz Investigation Synopsis

Sir:

Attached is the final draft of the Swartz investigation synopsis. If you have any questions feel free to contact me or ASAC (b)(6),(b)(7)(C) at 617/565-5640.

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service  
Boston Field Office  
617/565-5640

**FARON PARAMORE (GPA)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Wednesday, January 30, 2013 1:46 PM  
**To:** FARON PARAMORE (GPA)  
**Cc:** HUGH DUNLEAVY (INV)  
**Subject:** Fw: Final Draft of INV Requested Swartz Investigation Synopsis  
**Attachments:** Swartz INV Brief 1-29-2013.pdf

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Wednesday, January 30, 2013 09:53 AM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** FREDERICK SELLERS (INV)  
**Subject:** Final Draft of INV Requested Swartz Investigation Synopsis

Sir:

Attached is the final draft of the Swartz investigation synopsis. If you have any questions feel free to contact me or ASAIC (b)(6), (b)(7)(C) at 617/565-5640.

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service  
Boston Field Office  
617/565-5640

**FARON PARAMORE (GPA)**

---

**From:** FREDERICK SELLERS (INV)  
**Sent:** Wednesday, January 30, 2013 10:04 AM  
**To:** FARON PARAMORE (GPA)  
**Subject:** Fw: Final Draft of INV Requested Swartz Investigation Synopsis  
**Attachments:** Swartz INV Brief 1-29-2013.pdf

**FYI:**

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Wednesday, January 30, 2013 09:53 AM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** FREDERICK SELLERS (INV)  
**Subject:** Final Draft of INV Requested Swartz Investigation Synopsis

**Sir:**

Attached is the final draft of the Swartz investigation synopsis. If you have any questions feel free to contact me or  
ASAIC (b)(6), (b)(7)(C) at 617/565-5640.

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service  
Boston Field Office  
617/565-5640



**FARON PARAMORE (GPA)**

---

**From:** FREDERICK SELLERS (INV)  
**Sent:** Tuesday, January 29, 2013 5:36 PM  
**To:** FARON PARAMORE (GPA)  
**Subject:** FW: Aaron Swartz Case INV Request  
**Attachments:** Swartz INV Brief 1-29-2013.pdf

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Tuesday, January 29, 2013 4:59 PM  
**To:** dadinv; invsp  
**Cc:** HUGH DUNLEAVY (INV)  
**Subject:** FW: Aaron Swartz Case INV Request

---

**From:** JONATHAN BARTLETT (CID)  
**Sent:** Tuesday, January 29, 2013 4:06 PM  
**To:** HUGH DUNLEAVY (INV)  
**Subject:** FW: Aaron Swartz Case INV Request

---

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 29, 2013 4:04 PM  
**To:** JONATHAN BARTLETT (CID); EDWARD LOWERY (PID)  
**Subject:** FW: Aaron Swartz Case INV Request

---

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 29, 2013 3:23 PM  
**To:** (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)  
**Cc:** (b)(6),(b)(7)(C) (CID)  
**Subject:** Aaron Swartz Case INV Request

Good afternoon, Please see attachment.

Thank you,

SA (b)(6),(b)(7)(C)  
United States Secret Service  
Criminal Investigative Division  
(b)(6),(b)(7)(C) Direct  
(b)(6),(b)(7)(C) Mobile  
Email: (b)(6),(b)(7)(C) [uss.s.dhs.gov](mailto:(b)(6),(b)(7)(C)@uss.s.dhs.gov)

---

**From:** (b)(6),(b)(7)(C) (BOS)  
**Sent:** Tuesday, January 29, 2013 3:16 PM

**To:** (b)(6),(b)(7)(C) (CID)  
**Subject:** RE: Aaron Swartz Case

Please see attached

---

**From:** (b)(6),(b)(7)(C) CID)  
**Sent:** Wednesday, January 23, 2013 10:18 AM  
**To:** (b)(6),(b)(7)(C) (BOS)  
**Subject:** Aaron Swartz Case

Good morning, Can you please give me a call regarding the INV request that was sent to your office yesterday regarding the above case?

Thank you,

SA (b)(6),(b)(7)(C)  
United States Secret Service  
Criminal Investigative Division

(b)(6),(b)(7)(C) Direct  
Mobile  
Email: (b)(6),(b)(7)(C) usss.dhs.gov

## **FARON PARAMORE (GPA)**

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Tuesday, January 29, 2013 9:45 AM  
**To:** HUGH DUNLEAVY (INV); FREDERICK SELLERS (INV); JONATHAN BARTLETT (CID)  
**Cc:** DONNA CAHILL (LEG); LYNDIA WILLIAMS (GPA); (b)(6), (b)(7)(C) (GPA); (b)(6), (b)(7)(C) (GPA); (b)(6), (b)(7)(C) (GPA)  
**Subject:** House Oversight & Gov't Reform Committee (OGR) Chairman Issa Staff request briefing this Friday, February 1, 2013 at 1pm  
**Attachments:** Swartz Dismissal.pdf  
**Importance:** High

Good Morning, hope you are well.

Last night I was contacted by Mr. (b)(6), (b)(7)(C) Professional Staff with the House Oversight & Gov't Reform Committee (Chairman Issa staffer) requesting to receive a briefing from the USSS concerning our investigative efforts in the Aaron Swartz case in Boston. Mr. (b)(6), requested we provide the briefing this Friday, February 1, 2013 at 1pm in their office on Capitol Hill.

The attendees at the briefing will be staff from the offices of the Members who sit on the Oversight & Government Reform Committee. There could be as many as 20 staffers in the room.

Mr. (b)(6), had already been contacted by DOJ Office of Congressional Affairs and advised that they will provide a briefing at a TBD date in the future. I informed Mr. (b)(6), that we were aware that the U.S. Attorney's Office in Boston had already dismissed the charges against Mr. Swartz as he is now deceased. I further advised Mr. (b)(6), that we were still trying to clarify IF – IF there were any issues or concerns regarding the 6E material. Lastly, I informed Mr. (b)(6), that we would ONLY discuss our investigative efforts and that any questions that fell under the purview of DOJ (proffers / plea agreements/ etc.) would have to be directed / answered by DOJ.

Mr. (b)(6), advised that he understood the USSS would ONLY discuss the investigative aspects of this case.

Can INV please confirm your availability to provide the requested briefing this Friday, February 1, 2013 at 1pm.

Respectfully,

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

---

**From:** FREDERICK SELLERS (INV)  
**Sent:** Monday, January 28, 2013 12:13 PM  
**To:** FARON PARAMORE (GPA); HUGH DUNLEAVY (INV)  
**Subject:** FW: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

FYI:

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Monday, January 28, 2013 12:05 PM  
**To:** FREDERICK SELLERS (INV)  
**Subject:** RE: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

Sir - Please see attached, SR

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service  
Boston Field Office  
617/565-5640

---

**From:** FREDERICK SELLERS (INV)  
**Sent:** Monday, January 28, 2013 11:58 AM  
**To:** STEVEN RICCIARDI (BOS); HUGH DUNLEAVY (INV)  
**Cc:** FREDERICK SELLERS (INV)  
**Subject:** RE: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

Thanks Steve for the quick response. If possible, at your convenience, can we get a scanned copy of the dismissal to assist with any "potential" conversations with Chief Counsel?

Again - Thanks!

Fred Sellers

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Monday, January 28, 2013 11:26 AM  
**To:** HUGH DUNLEAVY (INV); FREDERICK SELLERS (INV)  
**Cc:** JONATHAN BARTLETT (CID); FARON PARAMORE (GPA); (b)(6),(b)(7)(C) (BOS)  
**Subject:** RE: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

Hugh & Fred:

I was advised that the charges have been dismissed, which is SOP, when a defendant is deceased prior to the completion of Judicial Action. I have a copy of the Dismissal order. In this case, Mr. Swartz was indicted (sealed) by a Grand Jury. Once there is an indictment it becomes public record, regulations regarding Rule 6E pertain just to the Grand Jury proceedings. (b)(5) Chief Counsel's Office (b)(5)

(b)(5) [redacted]  
chronological outline to you very soon.

Let me know if you need anything else, we should have the

Best regards - Steve

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service  
Boston Field Office  
617/563-5640

---

From: HUGH DUNLEAVY (INV)  
Sent: Monday, January 28, 2013 10:37 AM  
To: STEVEN RICCIARDI (BOS)  
Cc: HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID)  
Subject: Fw: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office  
Importance: High

Pls confirm

---

From: FARON PARAMORE (GPA)  
Sent: Monday, January 28, 2013 09:31 AM Eastern Standard Time  
To: HUGH DUNLEAVY (INV); FREDERICK SELLERS (INV); JONATHAN BARTLETT (CID)  
Cc: PAUL MORRISSEY (GPA); FARON PARAMORE (GPA); LYNDY WILLIAMS (GPA)  
Subject: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

Good Morning everyone, hope you are well.

Please see article below.

Looks like the US Attorney's Office in Boston dropped the charges against Aaron Swartz. Can we please have the Boston Field Office confirm this information.

If - If this is correct / true, this would also nullify our concerns regarding 6E material - I think.

Thanks. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

# **Feds drop charges against late Internet activist**

## **Aaron Swartz**

Federal prosecutors in Boston have dropped charges against Internet activist Aaron Swartz after his death.  
(Michael Francis McElroy / New York Times via Associated Press / January 30, 2009)  
By Jessica Guynn

January 14, 2013, 10:38 a.m.

Federal prosecutors in Boston have dropped charges against Internet activist Aaron Swartz.

Swartz, 26, was found dead Friday in his New York apartment. He apparently had hanged himself.

Prosecutors filed the notice of dismissal on Monday.

Swartz's family blamed his death on "prosecutorial overreach."

The U.S. attorney's office could not be reached for comment.

Federal prosecutors alleged Swartz used MIT's computers to illegally access millions of academic articles through the JSTOR database, a subscription service for scholarly articles. He was indicted in 2011 and was scheduled to go to trial on 13 counts including computer fraud. Swartz faced the possibility of millions of dollars in fines and up to 35 years in prison.

The case was seen as a showdown pitting the government and commercial interests against Internet "freedom fighters."

MIT President L. Rafael Reif on Sunday appointed Hal Abelson, a professor of computer science and engineering and a founding director of Creative Commons and the Free Software Foundation, to "lead a thorough analysis of MIT's involvement."

As news spread over the weekend of Swartz's death, the Web collectively mourned for a brilliant young technologist and activist who wanted to set the world's information free yet could never escape his own demons.

Confided one friend: "I'm not surprised that this is how his life ended, and I bet many others feel the same way. So sad, he had so much potential and not enough joy in his life."

Swartz was just 14 when he helped create RSS, a tool that distributes online content. He was one of the founders of the social news site Reddit, which was bought by Conde Nast. But he was best known as an activist for free and open access to the world's information.

"Everything he did was aimed at world-changing and at activism," said friend and historian Rick Perlstein.

Now his death is being used to question government's aggressive criminal prosecution of Internet activists.

Anonymous allegedly hacked MIT's website and left a tribute for Swartz: "We do not consign blame or responsibility upon MIT for what has happened, but call for all those feel heavy-hearted in their proximity to

this awful loss to acknowledge instead the responsibility they have — that we all have — to build and safeguard a future that would make Aaron proud."

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

AARON SWARTZ

Criminal No. 11-10260-NMG

**DISMISSAL**

Pursuant to FRCP 48(a), the United States Attorney for the District of Massachusetts, Carmen M. Ortiz, hereby dismisses the case presently pending against Defendant Aaron Swartz. In support of this dismissal, the government states that Mr. Swartz died on January 11, 2013.

Respectfully submitted,

1/14/13  
Date

Carmen M. Ortiz  
CARMEN M. ORTIZ  
United States Attorney

Stephen P. Heymann  
STEPHEN P. HEYMANN  
Assistant U.S. Attorney

Leave to File Granted:

Nathaniel M. Gorton 1/14/13  
Nathaniel M. Gorton, Judge  
United States District Court



## **FARON PARAMORE (GPA)**

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Monday, January 28, 2013 12:31 PM  
**To:** LYNDA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA);  
(b)(6),(b)(7)(C) (GPA); DONNA CAHILL (LEG)  
**Cc:** PAUL MORRISSEY (GPA)  
**Subject:** U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below.  
Can we have BFO confirm with AUSA's office  
**Attachments:** Swartz Dismissal.pdf

**FYI:**

Copy of the Swartz dismissal attached.

Just fyi. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

**Ph:** (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

---

**From:** FREDERICK SELLERS (INV)  
**Sent:** Monday, January 28, 2013 12:13 PM  
**To:** FARON PARAMORE (GPA); HUGH DUNLEAVY (INV)  
**Subject:** FW: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

**FYI:**

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Monday, January 28, 2013 12:05 PM  
**To:** FREDERICK SELLERS (INV)  
**Subject:** RE: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

Sir - Please see attached, SR

Steven D. Ricciardi  
Special Agent In Charge  
United States Secret Service  
Boston Field Office  
617/565-5640

---

**From:** FREDERICK SELLERS (INV)  
**Sent:** Monday, January 28, 2013 11:58 AM  
**To:** STEVEN RICCIARDI (BOS); HUGH DUNLEAVY (INV)  
**Cc:** FREDERICK SELLERS (INV)  
**Subject:** RE: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

Thanks Steve for the quick response. If possible, at your convenience, can we get a scanned copy of the dismissal to assist with any "potential" conversations with Chief Counsel?

Again --Thanks!

Fred Sellers

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Monday, January 28, 2013 11:26 AM  
**To:** HUGH DUNLEAVY (INV); FREDERICK SELLERS (INV)  
**Cc:** JONATHAN BARTLETT (CID); FARON PARAMORE (GPA) (b)(6),(b)(7)(C) (BOS)  
**Subject:** RE: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

Hugh & Fred:

I was advised that the charges have been dismissed, which is SOP, when a defendant is deceased prior to the completion of Judicial Action. I have a copy of the Dismissal order. In this case, Mr. Swartz was indicted (sealed) by a Grand Jury. Once there is an indictment it becomes public record, regulations regarding Rule 6E pertain just to the Grand Jury proceedings. (b)(5) Chief Counsel's Office (b)(5) (b)(5) Let me know if you need anything else, we should have the chronological outline to you very soon.

Best regards - Steve

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service  
Boston Field Office  
617/565-5640

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Monday, January 28, 2013 10:37 AM  
**To:** STEVEN RICCIARDI (BOS)  
**Cc:** HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID)  
**Subject:** Fw: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office  
**Importance:** High

Pls confirm

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Monday, January 28, 2013 09:31 AM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV); FREDERICK SELLERS (INV); JONATHAN BARTLETT (CID)  
**Cc:** PAUL MORRISSEY (GPA); FARON PARAMORE (GPA); LYNDY WILLIAMS (GPA)  
**Subject:** U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

Good Morning everyone, hope you are well.

Please see article below.

Looks like the US Attorney's Office in Boston dropped the charges against Aaron Swartz. Can we please have the Boston Field Office confirm this information.

If - If this is correct / true, this would also nullify our concerns regarding 6E material - I think.

Thanks. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(5) Direct line  
Cell  
(202) 406-5740 Fax

## **Feds drop charges against late Internet activist Aaron Swartz**

Federal prosecutors in Boston have dropped charges against Internet activist Aaron Swartz after his death.  
(Michael Francis McElroy / New York Times via Associated Press / January 30, 2009)  
By Jessica Guynn

January 14, 2013, 10:38 a.m.

Federal prosecutors in Boston have dropped charges against Internet activist Aaron Swartz.

Swartz, 26, was found dead Friday in his New York apartment. He apparently had hanged himself.

Prosecutors filed the notice of dismissal on Monday.

Swartz's family blamed his death on "prosecutorial overreach."

The U.S. attorney's office could not be reached for comment.

Federal prosecutors alleged Swartz used MIT's computers to illegally access millions of academic articles through the JSTOR database, a subscription service for scholarly articles. He was indicted in 2011 and was scheduled to go to trial on 13 counts including computer fraud. Swartz faced the possibility of millions of dollars in fines and up to 35 years in prison.

The case was seen as a showdown pitting the government and commercial interests against Internet "freedom fighters."

MIT President L. Rafael Reif on Sunday appointed Hal Abelson, a professor of computer science and engineering and a founding director of Creative Commons and the Free Software Foundation, to "lead a thorough analysis of MIT's involvement."

As news spread over the weekend of Swartz's death, the Web collectively mourned for a brilliant young technologist and activist who wanted to set the world's information free yet could never escape his own demons.

Confided one friend: "I'm not surprised that this is how his life ended, and I bet many others feel the same way. So sad, he had so much potential and not enough joy in his life."

Swartz was just 14 when he helped create RSS, a tool that distributes online content. He was one of the founders of the social news site Reddit, which was bought by Conde Nast. But he was best known as an activist for free and open access to the world's information.

"Everything he did was aimed at world-changing and at activism," said friend and historian Rick Perlestein.

Now his death is being used to question government's aggressive criminal prosecution of Internet activists.

Anonymous allegedly hacked MIT's website and left a tribute for Swartz: "We do not consign blame or responsibility upon MIT for what has happened, but call for all those feel heavy-hearted in their proximity to this awful loss to acknowledge instead the responsibility they have — that we all have — to build and safeguard a future that would make Aaron proud."

## **FARON PARAMORE (GPA)**

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Tuesday, January 22, 2013 1:05 PM  
**To:** PAUL MORRISSEY (GPA); JANE MURPHY (INV); HUGH DUNLEAVY (INV)  
**Cc:** FARON PARAMORE (GPA); LYNDIA WILLIAMS (GPA)  
**Subject:** Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee

Good afternoon, hope you are well.

Consult with outside agency.

Thanks much.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

## **FARON PARAMORE (GPA)**

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Tuesday, January 22, 2013 10:59 AM  
**To:** (b)(6),(b)(7)(C) @usdoj.gov  
**Cc:** (b)(6),(b)(7)(C) @hq.dhs.gov  
**Subject:** U.S. Secret Service - Aaron Swartz case out of Boston

Good Morning Ms (b)(6),(b)(7)(C) hope you are well.

Ma'am, my name is Faron K. Paramore. I serve as the Deputy Assistant Director in the Office of Congressional Affairs for the U.S. Secret Service.

Last Thursday afternoon (1/17/13) I was contacted by a Mr. (b)(6),(b)(7)(C) professional staff with the House Oversight & Government Reform Committee (Majority Staff - Chairman Issa), requesting to receive a briefing from the U.S. Secret Service regarding our role / investigation of the Aaron Swartz case out of Boston, MA.

Ma'am, at your convenience would it be possible for me to give you a call to discuss this matter.

Thank you very much for your time.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

Note the Issa comments towards the end of the article <http://thehill.com/blogs/hillicon-valley/technology/277709-justice-department-defends-prosecution-of-activist-swartz>

• Previous TJX hacking case - Same prosecutor and the suspect also committed suicide:

<http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html>

## **FARON PARAMORE (GPA)**

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Friday, January 18, 2013 3:40 PM  
**To:** (b)(6),(b)(7)(C) dhq.dhs.gov  
**Cc:** FARON PARAMORE (GPA)  
**Subject:** From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers  
**Attachments:** Clips Extra January 14 2013.doc; Clips Extra January 15 2013.doc; Doc1.doc

Good afternoon (b)(6),(b) hope you are well.

(b)(6),(b) just left you a v/a.

Over the last year and a half our Boston Field Office / New England Electronics Crimes Task Force was working a cyber case. Our Suspect was a Mr. Aaron Swartz's. Long story short -- Swartz killed himself about a week ago. His federal trial was suppose to start in a month or so.

NOW, there have been numerous articles on the web about how the "Federal Gov't" was heavy handed in this case.

Late yesterday afternoon I received a call from Chairman Issa's staff requesting to receive a briefing possible next week.

Want to make sure DHS is in the loop on what actually happened.

Also, we will need to coordinate with DOJ Congressional Affairs on this. The USSS will ONLY speak to our role in this case. DOJ (The U.S. Attorney's Office has a big part in this also).

Please give me a call when you have a moment so I can brief you.

See links below.

Thanks. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

---

**From:** (b)(6),(b)(7)(C) GPA)  
**Sent:** Thursday, January 17, 2013 1:46 PM  
**To:** FARON PARAMORE (GPA)  
**Cc:** LYNDIA WILLIAMS (GPA) (b)(6),(b)(7)(C) (GPA) (b)(6),(b)(7)(C) (GPA) (b)(6),(b)(7)(C) (GPA)  
**Subject:** FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Faron,

Here are some -- see attached.

Also - Here are a couple more things that (b)(6),(b)(7)(C) found:

- Note the Issa comments towards the end of the article  
<http://thehill.com/blogs/hillicon-valley/technology/277709-justice-department-defends-prosecution-of-activist-swartz>

- Previous TJX hacking case - Same prosecutor and the suspect also committed suicide:

<http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html>

Let us know what else you need.

Thanks,

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

-----Original Message-----

From: (b)(6),(b)(7)(C) (GPA)

Sent: Thursday, January 17, 2013 1:39 PM

To: (b)(6),(b)(7)(C) (GPA)

Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

<http://crooksandliars.com/karol1/unanswered-question-why-was-secret-service->

<http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html>

-----Original Message-----

From: FARON PARAMORE (GPA)

Sent: Thursday, January 17, 2013 1:35 PM

To: (b)(6),(b)(7)(C) (GPA)

Cc: LYNDIA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA)

Subject: FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

(b)(6),(b)(7) can you pull down any / all articles you can find on the internet concerning this guy

Mr. Aaron Swartz.

Issa's office just called and are looking for a briefing tbd time next week.

Thx. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
(b)(6),(b)(7)(C) Cell  
(202) 406-5740 Fax

-----Original Message-----

From: EDWIN DONOVAN (GPA)



Sent: Thursday, January 17, 2013 12:54 PM

To: HUGH DUNLEAVY (INV); JANE MURPHY (INV); PAUL MORRISSEY (GPA); LEE FIELDS (INV); JONATHAN BARTLETT (CID)

Cc: (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); FARON PARAMORE (GPA); (b)(6),(b)(7)(C) (GPA); LYNDIA WILLIAMS (GPA)

Subject: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Attached is an article from Time.com discussing Aaron Swartz's suicide and reaction from some members of Congress.

Link to article: <http://business.time.com/2013/01/16/aaron-swartzs-suicide-triggers-response-from-us-lawmakers/>

**FARON PARAMORE (GPA)**

---

**From:** (b)(6),(b)(7)(C) (GPA)  
**Sent:** Thursday, January 17, 2013 1:46 PM  
**To:** FARON PARAMORE (GPA)  
**Cc:** LYNDIA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA)  
**Subject:** FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers  
**Attachments:** Clips Extra January 14 2013.doc; Clips Extra January 15 2013.doc; Doc1.doc

Faron,

Here are some -- see attached.

Also - Here are a couple more things that (b)(6), (b)(7)(C) found:

- Note the Issa comments towards the end of the article  
<http://thehill.com/blogs/hillicon-valley/technology/277709-justice-department-defends-prosecution-of-activist-swartz>
- Previous TJX hacking case - Same prosecutor and the suspect also committed suicide:  
<http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html>

Let us know what else you need.

Thanks,

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

-----Original Message-----

**From:** (b)(6),(b)(7)(C) (GPA)  
**Sent:** Thursday, January 17, 2013 1:39 PM  
**To:** (b)(6),(b)(7)(C) (GPA)  
**Subject:** FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers  
<http://crooksandliars.com/karoli/unanswered-question-why-was-secret-service->

<http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html>

-----Original Message-----

**From:** FARON PARAMORE (GPA)  
**Sent:** Thursday, January 17, 2013 1:35 PM  
**To:** (b)(6),(b)(7)(C) (GPA)  
**Cc:** LYNDIA WILLIAMS (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA)  
**Subject:** FW: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

(b)(6),(b)(7)(C) can you pull down any / all articles you can find on the internet concerning this guy

Mr. Aaron Swartz.

Issa's office just called and are looking for a briefing tbd time next week.

Thx. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5748 Fax

-----Original Message-----

From: EDWIN DONOVAN (GPA)  
Sent: Thursday, January 17, 2013 12:54 PM  
To: HUGH DUNLEAVY (INV); JANE MURPHY (INV); PAUL MORRISSEY (GPA); LEE FIELDS (INV); JONATHAN BARTLETT (CID)  
Cc: (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); (b)(6),(b)(7)(C) (GPA); FARON PARAMORE (GPA); (b)(6),(b)(7)(C) (GPA); LYNDIA WILLIAMS (GPA)  
Subject: From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers

Attached is an article from Time.com discussing Aaron Swartz's suicide and reaction from some members of Congress.

Link to article: <http://business.time.com/2013/01/16/aaron-swartzs-suicide-triggers-response-from-us-lawmakers/>

**FARON PARAMORE (GPA)**

---

**From:** EDWIN DONOVAN (GPA)  
**Sent:** Thursday, January 17, 2013 12:54 PM  
**To:** HUGH DUNLEAVY (INV); JANE MURPHY (INV); PAUL MORRISSEY (GPA); LEE FIELDS (INV); JONATHAN BARTLETT (CID)  
**Cc:** (b)(6),(b)(7)(C) [GPA]; (b)(6),(b)(7)(C) [GPA]; (b)(6),(b)(7)(C) [GPA]; (b)(6),(b)(7)(C) [GPA]; FARON PARAMORE (GPA); LYNDIA WILLIAMS (GPA)  
**Subject:** From Time.com: Aaron Swartz's Suicide Triggers Response from Top U.S. Lawmakers  
**Attachments:** Doc1.doc

Attached is an article from Time.com discussing Aaron Swartz's suicide and reaction from some members of Congress.

Link to article: <http://business.time.com/2013/01/16/aaron-swartzs-suicide-triggers-response-from-us-lawmakers/>

FROM TIME.COM

Aaron Swartz, the brilliant and mercurial young programmer who killed himself in Brooklyn last Friday, was memorialized in his hometown of Highland Park, Ill., Tuesday, as the shockwaves from his death reached Washington, D.C.

As Swartz's family and friends were grieving in Chicago, several Capitol Hill lawmakers expressed sadness and confusion over his death. One prominent U.S. lawmaker, Zoe Lofgren (D-Calif.), said she would introduce reforms to change the federal law at the heart of the case.

In a bill called "Aaron's Law," Lofgren aims to amend the Computer Fraud and Abuse Act (CFAA), which Massachusetts prosecutors used to charge Swartz with over 30 years in prison. Swartz's family has accused the Massachusetts U.S. Attorney's office with hounding the young activist over what they call a "victimless crime." Specifically, Lofgren's bill would amend the existing law to distinguish between a terms of service violation and a federal data theft crime.

"Lofgren's bill is a good start," Harvard professor Lawrence Lessig told TIME in a phone interview Wednesday morning. Lessig eulogized Swartz at the funeral Tuesday. Like many of Swartz's friends, Lessig hopes that something positive will come out of the young programmer's passing, he said.

"The CFAA was the hook for the government's bullying," Lessig wrote on Reddit, the hugely popular Internet activist hub that Swartz helped launch. "This law would remove that hook. In a single line: no longer would it be a felony to breach a contract. Let's get this done for Aaron — now." (Read Lofgren's bill here.)

(MORE: Aaron Swartz's Suicide Prompts MIT Soul-Searching)

Swartz faced over 30 years in prison on federal data-theft charges for downloading articles from the subscription-based academic research service JSTOR. In 2011, Swartz allegedly broke into a secure MIT computer closet and hooked up a laptop in order to download JSTOR files, before he was arrested by local authorities. JSTOR later settled its civil complaint with Swartz, but MIT did not follow suit, giving Massachusetts federal prosecutors the implicit green light to go ahead with the prosecution, Lessig says.

"The charges were ridiculous and trumped-up," Rep. Jared Polis (D-Colo.) told The Hill newspaper. "It's absurd that he was made a scapegoat. I would hope that this doesn't happen to anyone else." Polis called Swartz — who co-authored an early version of the popular Internet tool RSS at age 14 and would later become an early leader of Reddit — a "martyr."

At the funeral, Swartz's father Robert Swartz said his son was "killed by the government, and MIT betrayed all of its basic principles," according to the Associated Press. On Sunday, MIT president L. Rafael Reif announced an internal investigation into the school's involvement in

Swartz's suicide. Reif has asked Hal Abelson, a respected MIT professor, and a founding director of Creative Commons and the Free Software Foundation, to lead the probe.

House Oversight Committee Chairman Darrell Issa (R-Calif.) said he has opened an investigation of the Justice Department's case against Aaron Swartz, according to HuffPost. "I'm not condoning his hacking, but he's certainly someone who worked very hard," Issa told the news website.

"Had he been a journalist and taken that same material that he gained from MIT, he would have been praised for it. It would have been like the Pentagon Papers." (Not exactly: The Pentagon Papers were classified federal government documents. Swartz was accused of accessing scholarly articles on a university network.)

**(MORE: Aaron Swartz, Tech Prodigy and Internet Activist, Is Dead at 26)**

Rep. Issa, the chairman of the House Judiciary Committee, is a shrewd political operator who has worked with Internet activists in the past. Last year, Rep. Issa was instrumental in the defeat of controversial anti-piracy legislation, which Swartz worked to oppose. A conservative Republican, Issa has sensed the recent groundswell of Internet-based activism, and sought to align himself with it. Issa has made investigating U.S. government "over-reaching" a key part of his agenda.

Meanwhile, incoming Massachusetts senator Elizabeth Warren issued a statement praising Swartz. "When I met Aaron Swartz in 2010, I discovered a young man who was passionate, sharp, a little shy, and, above all, warm and good natured," Warren said in a statement to HuffPost. "He seemed like the kind of person who couldn't hurt a fly — he just had that kind of presence. Aaron made remarkable contributions to our world, and his advocacy for Internet freedom, social justice, and Wall Street reform demonstrated both the power of his ideas and the depth of his commitment. The world is a poorer place without Aaron."

In statement on Reddit, Rep. Lofgren said she wants to reform the Computer Fraud and Abuse Act (CFAA) in order to "prevent what happened to Aaron from happening to other Internet users." Lofgren, who represents Silicon Valley, is an outspoken voice on technology issues in the U.S. Congress.

"The government was able to bring such disproportionate charges against Aaron because of the broad scope of the wire fraud statute," Lofgren said. "It looks like the government used the vague wording of those laws to claim that violating an online service's user agreement or terms of service is a violation of the CFAA and the wire fraud statute."

Assistant U.S. Attorney Stephen Heymann, who works for Massachusetts U.S. Attorney Carmen Ortiz, has faced criticism over his handling of the case. According to Swartz's lawyer, Elliot Peters, Heymann was aiming for a "juicy looking computer crime cases and Aaron's case, sadly for Aaron, fit the bill," Peters told HuffPost. Peters told the website that he thought Heymann believed the Swartz case "was going to receive press and he was going to be a tough guy and read his name in the newspaper."

Read more: <http://business.time.com/2013/01/16/aaron-swartzs-suicide-triggers-response-from-us-lawmakers/#ixzz2IFtES9y9>

**RIF**

At 19:35 hours Friday, January 11, 2013, it was reported to NYPD that Aaron Swartz had committed suicide. Detective (b)(6), (b)(7)(C) of Precinct 71 responded to (b)(6), (b)(7)(C) (b) 11225. (b)(6), (b)(7)(C) Swartz' (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)

Aaron Swartz was identified and all indications thus far reveal that it was a suicide. (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)

No note was left but there were computers in the apartment. Due to dual ownership claims and no apparent foul play, the computers on scene were not seized.

The New York Medical Examiner's Office has listed it as an open case at this time.

Aaron Swartz was very outspoken that he suffered with depression and even wrote blog entries articulating suicide. He literally was a child prodigy and was clearly brilliant. He wrote script (source-code) that was purchased when he was 14 years old for \$ 4 million dollars and a few years later he wrote another code which Norton Antivirus purchased for \$ 1.5 million dollars. In 2008 he became politically active in cyber related activities, he authored the Guerilla Manifesto. The original website for this manifesto was removed by Aaron Swartz from his website shortly after his arrest; basically because it was a written motive to the crimes he was subsequently charged with.

This case was initiated in the Boston Field Office on January 4, 2011 when Detective (b)(6), (b)(7)(C) of Cambridge Police Department (full time member of the New England Electronic Crimes Task Force (NEECTF) who resides in the Boston Field Office on a daily basis) received a telephone call from the MIT Police stating there was an unauthorized laptop computer located in a computer closet on campus attached to a switch on the MIT network. The trial was scheduled to begin April 1, 2013 with suppression motions occurring January 25, 2013. During the past two years of litigation, Swartz went through three of the top defense counsel teams finally ending with Elliot Peters (who recently successfully defended Lance Armstrong in his doping case) of California.

The following is a copy of the synopsis of the facts presented by the U.S. Attorneys' Office in response to the defense council's filing for the suppression hearing:

Late during the night of September 24, 2010, an individual registered his computer on MIT's campus and obtained a guest account on MIT's computer network. The individual did not provide his true identity at this or any subsequent time, and neither MIT personnel nor law enforcement officers knew the individual's name until his arrest months later. The individual registered his computer by specifying his name as "Gary Host," a pseudonym, and his e-mail address as ghost@mailinator.com, a disposable e-mail address by virtue of its requiring no initial e-mail registration and keeping no records of e-mail access.<sup>3</sup> Before assigning the computer an



IP address, MIT's network automatically collected the computer's owner-created name — "ghost laptop" — and the unique identifying number associated with the computer's Internet networking hardware, known as the computer's Media Access Control or "MAC" address.

These are standard login and communication procedures.

MIT's DHCP4 computer server then used a standard Internet protocol to assign the individual an IP address (18.55.6.215) for use while on the network. The network kept records of the computer's registration information, its IP address, and its MAC address. These records are standard computer-networking records, and did not include any computer commands that the individual typed in or ran, or any data that the computer downloaded. (Exs. 6, 7).

3 Mailinator advertised itself as a free e-mail service that would accept mail for any email address directed to mailinator.com without need for a prior registration or account; would automatically delete all e-mail after several hours, whether read or not; and would keep no logs (records) of e-mail access.

4 DHCP is the acronym for Dynamic Host Configuration Protocol.

On September 25, 2010, the day after registering the "ghost laptop," the individual used the "ghost laptop" to systematically access and rapidly download an extraordinary volume of articles from JSTOR by using a software program that sidestepped JSTOR's computerized limits on the volume of each user's downloads. The downloads and requests for downloads were so numerous, rapid, and massive that they impaired the performance of JSTOR's computers.

As JSTOR, and then MIT, became aware of these downloads and problems, both attempted to block the individual's computer from further communications. On the evening of September 25, 2010, after suffering hundreds of thousands of downloads from the ghost laptop, JSTOR temporarily ended the downloads by blocking network access from the computer at IP address 18.55.6.215.

The next day, however, the ghost laptop's user obtained a new IP address from MIT's

network, changing the last digit in its IP address by one from 18.55.6.215 to 18.55.6.216. This defeated JSTOR's IP address block, enabling the ghost laptop to resume furiously downloading articles from JSTOR. This downloading continued until the middle of September 26, when JSTOR spotted it and blocked communication from IP address 18.55.6.216 as well.

The September 25 and 26 downloads had impaired JSTOR's computers and misappropriated significant portions of its archive. Because the download requests had originated from two MIT IP addresses that had begun with 18.55.6 — that is, 18.55.6.215 and 18.55.6.216 — JSTOR began blocking a broader range of MIT IP addresses on September 26. The new block prevented MIT researchers assigned MIT IP addresses 18.55.6.0 through 18.55.6.255 (as many as 253 computers) from performing research through JSTOR's archive for three to four days.

Moreover, when JSTOR notified MIT of the problems, MIT, too, banned the "ghost laptop" from using its network. To do this, MIT terminated the ghost laptop's guest registration on September 27, 2010, and prohibited the computer, as identified by its hardware MAC address, from being assigned a new IP address again through the guest registration process.

On October 2, 2010, less than a week after JSTOR and MIT had barred the individual's ghost laptop from communicating with their networks, the individual obtained yet another guest connection for the ghost laptop on MIT's network. Having recognized that MIT or JSTOR had blocked his ghost laptop by recognizing its MAC address, the individual now manipulated the ghost laptop's MAC address to mislead MIT into believing that he was a new and different guest registrant.

Six days later, the individual connected a second computer to MIT's network and created another guest account using pseudonyms similar to those he had used with the "ghost laptop": he registered the new computer under the name "Grace Host", a temporary email address of ghost42@mailinator.com, and a computer client name of "ghost macbook."

On October 9, 2010, the individual activated the ghost laptop and the ghost macbook to download JSTOR's articles once again. The downloads came so fast and numerous that the individual again significantly impaired the operation of some of JSTOR's computers.

Once again, MIT could not identify who was controlling these computers or where they were physically located, and JSTOR could not isolate the interloper to a consistent IP address

5 A computer's MAC address is initially assigned by an equipment manufacturer, but can be misrepresented electronically by a knowledgeable user. The user altered the ghost laptop's MAC address to appear as 00:23:5a:73:5f:fc rather than the prior MAC address of

00:23:5a:73:5f:fb. that could be blocked. Consequently, JSTOR blocked access by every computer using an MIT IP address campus-wide for approximately three days, again depriving legitimate MIT users from accessing JSTOR's services. And MIT blocked computers using the ghost laptop's and the ghost macbook's MAC addresses as well.

Nevertheless, between the end of October and January 6, 2011, the hacker obtained at least three new IP addresses and assigned his computer two new MAC addresses. He also moderated the speed of the downloads, which made them less noticeable to JSTOR. The exfiltration of JSTOR's collection was nonetheless extreme: over this period, the individual downloaded well over a million of JSTOR's articles.

Because the hacker had modified the speed of his downloads, JSTOR did not notice his latest downloads until around Christmas, 2010. Once noticed, however, JSTOR provided MIT with the hacker's latest IP address. Now that MIT's network security personnel had a more robust set of network tools, they could consult network traffic routing records and trace the IP address back to a concrete physical location on campus.

So on January 4, 2011, an MIT network security analyst traced the hacker's IP address to a network switch located in a basement wiring closet in MIT's Building 16. Building 16's street level doors have no-trespassing signs posted on them. (Ex. 8). The wiring closet is protected by

a pair of locked steel doors. (Ex. 9). The closet is generally locked, but at that time its lock could be forced by a quick jerk of its double doors. When MIT personnel entered the closet, they found a cardboard box with a wire leading from it to a computer network switch. (Ex. 10).<sup>6</sup> MIT personnel removed the box from the laptop at first, and then MIT personnel or law enforcement officers replaced the box on one or more occasions. The second photograph was taken after the box was replaced, not when it was initially found.

<sup>7</sup> Hidden under the box was the ghost laptop, an Acer-brand laptop, connected to a separate hard drive for excess storage. (Ex. 11). The network cable connected the laptop to the network switch, thus giving the laptop Internet access. (Ex. 12). The laptop's direct connection to the network switch was unusual because MIT does not connect computers directly to those switches. MIT called campus police to the scene, who, in turn, brought in the Cambridge Police and the Secret Service. Over the course of the morning and early afternoon of January 4th, MIT and law enforcement officers collaboratively took several steps to identify the perpetrator and learn what he was up to:

- (1) Cambridge Police crime scene specialists fingerprinted the laptop's interior and exterior and the external hard drive and its enclosure;
- (2) MIT placed and operated a video camera inside the closet, which, as discussed below, later recorded the hacker (subsequently identified as Aaron Swartz) entering the wiring closet and performing tasks within it;
- (3) The Secret Service opened the laptop and sought to make a copy of its volatile memory (RAM), which would automatically be destroyed when the laptop's power was turned off, but the effort resulted in their seeing only the laptop's user sign-in screen;
- (4) MIT connected a second laptop to the network switch in order to record the laptop's communications, a type of recording often referred to as a "packet capture;" the Secret Service subsequently concurred with the packet capture, none of which was turned over to officers until MIT was issued a subpoena after Swartz's arrest;
- (5) Beginning on January 4, 2011, MIT agreed to provide, and later provided, the Secret Service copies of network logs pertaining to

<sup>7</sup> From the time of law enforcement's arrival on January 4, 2011, through the suspect's

arrest and identification on January 6, 2011, the effort by MIT and law enforcement to identify the individual was both consensual and collaborative.

8 This second laptop is seen on a chair in Ex. 10.8 the ghost laptop and ghost macbook between September 24, 2010 and January 6, 2011, (b)(3) Rule 6E

(b)(3) Rule 6E

9 By mid-day on January 4th, MIT and law enforcement personnel had completed their initial crime scene investigation. Experience told them that merely removing the hacker's computer equipment would just result in his renewing his efforts elsewhere. So, rather than take the hacker's equipment away, MIT and law enforcement instead restored the closet to its initial appearance upon discovery, and monitored who entered it and handled the laptop. In this way, the hacker would not necessarily know that his criminal tools had been discovered, his identity might be uncovered, and he could be stopped.

The ruse worked. Within an hour of their departure, the hacker returned. After entering the wiring closet and shutting the doors behind him, (Ex. 13), the hacker replaced the hard drive connected to the laptop with a new one he took from his backpack, and then concealed his equipment once again underneath the cardboard box.

Two days later, on January 6, 2011, the hacker returned to the wiring closet yet again.

This time, worried about being identified, the hacker covered his face with his bicycle helmet as he entered the closet. (Ex. 14). Once inside and with the door closed, the hacker disconnected the laptop and placed it, the external hard drive, and the network cable in his backpack. (Ex. 15).

As he left, he again hid his face with his bicycle helmet. (Ex. 16).

By January 6, 2011, the hacker had downloaded a major portion of the 6 to 7 million articles then contained in JSTOR's digitized database.

As discussed below, both the law and MIT's policies and procedures allowed MIT to turn these records over consensually, but it also could, and at points did, insist upon a subpoena.

A little after 2:00 that afternoon, MIT Police (b)(6), (b)(7)(C) who had been

involved in the investigation, was heading down Massachusetts Avenue within a mile of MIT when he spotted a bicyclist who looked like the hacker caught on the wiring closet video.

(b)(6),(b)(7)(C) identified himself as a police officer. After a brief exchange, the individual dropped his bike to the ground and ran away. The individual was chased, apprehended, arrested, and identified as Aaron Swartz. During a search incident to arrest, Cambridge police found a USB storage drive in Swartz's backpack, which they seized and stored as evidence.

Approximately an hour later, MIT technical staff used computer routing and addressing records to locate Swartz's ghost laptop and hard drive in the Student Information Processing Board's office in MIT's student center. Law enforcement found the equipment on the floor under a desk. (Ex. 17). The equipment was subsequently seized and stored as evidence by Cambridge Police.

Aaron Swartz was charged by the Commonwealth in a criminal complaint alleging breaking and entering into MIT's property with intent to commit a felony, and was subsequently indicted by a Massachusetts grand jury for the same charge along with stealing JSTOR's electronically processed or stored data, and accessing a computer system without authorization.

While the Commonwealth pursued state charges, the U.S. Attorney's Office began a separate investigation on January 5, 2011. On February 9, 2011, the Secret Service obtained a warrant to search Swartz's apartment, followed by a warrant to search his office on February 11, 2011. Both were executed on February 11th. Also on February 9, 2011, the Secret Service obtained warrants to seize from the Cambridge Police and then search the laptop, the hard drive, and the USB storage device. These warrants were returned unexecuted and new warrants were obtained on February 24, 2011. On May 16, 2011, Swartz was served with a forfeiture warrant for property of JSTOR in his possession and refused to comply with the Court's warrant.<sup>10</sup> Swartz was indicted federally for wire fraud, computer fraud, and data theft, which was followed by the present Superseding Indictment on the same theories.

<http://www.rollingstone.com/politics/news/why-did-the-justice-system-target-aaron-swartz-20130123>

## Why Did the Justice System Target Aaron Swartz?

**26-year-old Internet activist's tragic suicide raises questions about prosecutorial overreach**

By Steven Hsieh

**Rolling Stone Magazine**

January 23, 2013 3:49 PM ET

Hundreds of mourners filled the Great Hall at New York's Cooper Union on January 19th to honor the life of Aaron Swartz, the Internet activist who took his own life earlier this month at age 26.

Swartz was well-known in technology circles for helping develop the RSS web feed format and the popular site Reddit, among other accomplishments. At the time of his death, he was facing 13 felony charges and up to 50 years in prison: Prosecutors had accused him of using MIT's network to download too many scholarly articles from an academic database called JSTOR.

Swartz's friends and family have said they believe he was driven to his death by a justice system that hounded him needlessly over an alleged crime with no real victims. "[He was] forced by the government to spend every fiber of his being on this damnable, senseless trial," his partner Taren Stinebrickner-Kauffman said at the memorial, "with no guarantee that he could exonerate himself at the end of it."

Swartz's tragic death has already begun forcing lawmakers to start rethinking our draconian computer laws. And House Oversight Committee Chairman Darrell Issa (R-California) even promised an investigation of the Justice Department prosecutors who did their best to send a young Internet pioneer to prison.

Two zealous federal prosecutors handled Swartz's case: U.S. district attorney Carmen Ortiz and assistant attorney Stephen Heymann. In the days after his death, writers, tech experts, and many of Swartz's friends have called out Heymann and Ortiz for prosecutorial overreach. A White House petition demanding the removal of Ortiz garnered well over 25,000 signatures, reaching the level which guarantees an eventual response from the Obama administration.

Some of Swartz's advocates believe the prosecution sought excessive punishment to set an example in the age of Wikileaks and Anonymous.

"This was, in my opinion, part of a coordinated campaign to scare young Internet activists," says Roy Singham, ThoughtWorks chairman and a friend of Swartz.

It's worth reviewing the so-called crime which put Swartz in the government's crosshairs. From September 24th, 2010 to January 6th, 2011, he accessed MIT's network to scrape an "extraordinary volume of articles" from the academic database JSTOR. Initially, he used the university's open wireless network to grab the files. But after several attempts by JSTOR and MIT to block him, Swartz gained access to a restricted closet and directly hardwired his laptop to the network, leaving it there to pull data.

MIT personnel found Swartz's laptop on the morning of January 4th, 2011, and connected a second computer to the network switch to monitor Swartz's activity. They also fingerprinted Swartz's device and installed a camera in the closet to identify their culprit.

On the same day, the U.S. Secret Service took over the investigation. Court documents reveal that Secret Service agent Michael Prickett recommended MIT personnel leave Swartz's laptop in the closet for monitoring. All acquired data was eventually disclosed to the Secret Service.

On January 6th, 2011, MIT and Cambridge police, with the help of special agent Prickett, arrested Swartz on charges of breaking and entering with intent to commit a felony. As blogger Marcy Wheeler suggests, the early involvement of the Secret Service "makes it clear that this was a nationally directed effort to take down Swartz."

JSTOR chose not to pursue charges against Aaron Swartz – who not only returned all downloaded content, but also ensured it "was not and would not be used, copied, transferred or distributed." That didn't stop MIT and the feds from indicting Swartz on 13 felony charges and insisting on prison time.

Ortiz and Heymann charged Swartz under the Computer Fraud and Abuse Act, a 29-year-old law, notorious in the legal world for being broadly interpretable. They argued that Swartz accessed MIT and JSTOR computers without "authorization," despite MIT's extraordinarily open network policy and Swartz's legal access to JSTOR content.

Despite admitting that Swartz wasn't financially motivated by his act – and even after learning that the 26-year-old had battled depression – Ortiz and Heymann refused to offer a deal that didn't include at least six months of prison time and a guilty plea on all 13 charges. If Swartz chose not to label himself a felon for life, he'd risk the possibility of many years in the slammer.

Any probe into this case must raise serious questions about prosecutorial overreach by Ortiz and Heymann. Heymann's record, in particular, reeks of bullying and power-



hungry ambition. A damning report from the Huffington Post paints the assistant U.S. attorney – and head of his court's computer crimes task force – as a careerist who sought tough convictions to bolster his reputation. In 2008, Heymann prosecuted another hacking case that ended with a suicide.

But holding Heymann and Ortiz accountable, while necessary, won't be enough to stop the persecution of Internet activists and hacking culture in this country. It's time to have a serious conversation over whether Swartz's fight for free information truly warranted Secret Service investigation. Should participating in a DDoS attack, the Internet's equivalent of a sit-down strike, send someone to 30 months in prison? As Harvard professor Lawrence Lessig has put it, our government pursued Swartz as if he were a "9/11 terrorist."

Last month, Rolling Stone's Matt Taibbi noted the absurdity of HSBC bankers skating on serious drug money laundering charges while hundreds of thousands of Americans sit behind bars for petty drug offenses. The Secret Service's involvement in hunting down a 26-year-old charged with downloading too many scholarly articles is just another example of our justice system's chillingly warped priorities.

## **FIELD ACTIVITIES:**

### **Boston Field Office**

#### **New England Electronic Crimes Task Force**

#### **MIT Network Intrusion Results in Federal Indictment and Arrest**

On January 4, 2011, Massachusetts Institute of Technology (MIT) Police Department contacted the Boston Field Office and requested assistance from the New England Electronic Crimes Task Force (NEECTF) regarding an investigation into a network intrusion. The initial investigation identified Aaron Swartz as the primary suspect.

NEECTF agents determined that Aaron Swartz intruded into the MIT network without authorization. Swartz broke into a locked closet containing network components, connected his computer to the MIT computer network and downloaded documents from a not-for-profit archive of scientific journals and academic work, known as "JSTOR." Swartz avoided MIT's and JSTOR's electronic security and distributed a significant amount of JSTOR's archive through one or more file-sharing sites. Through investigative interviews and electronic forensic evidence, agents established that Swartz's un-authorized access impaired MIT computers, disabled servers, and deprived various JSTOR users from accessing research. Agents discovered JSTOR and MIT were unable to block Swartz's attacks, as Swartz continued his intrusions utilizing new methods for accessing JSTOR. Subsequently Swartz exploited MIT's computer system to steal over four million articles from JSTOR.

On July 14, 2011, Aaron Swartz was indicted in U.S. District Court, District of Massachusetts, charged with violations of Title 18, United States Code, Sections 2 (Aiding and Abetting), 1030a2 (Theft of Information From a Computer), 1030 a5B (Recklessly Damaging a Computer) and 1343 (Wire Fraud).

On July 19, 2011, Swartz surrendered to federal authorities and was arraigned before Magistrate Judge Judith G. Dein and released on \$100,000 bond.

On November 17, 2011, Swartz was also indicted in Middlesex Superior Court for breaking and entering in the daytime with intent to commit a felony, larceny over \$250 and unauthorized access to a computer network.

On November 30, 2011, Swartz was arraigned in Middlesex Superior Court for breaking and entering daytime, larceny over \$250 and unauthorized access to a computer network.

On November 12, 2012, a superseding indictment was rendered in the U.S. District Court, District of Massachusetts, for violations of Title 18, United States Code, Sections 2 (Aiding and Abetting), 1030 (Computer Fraud – unlawfully obtaining information from a protected computer and recklessly damaging a protected computer) and 1343 (Wire Fraud).

From November 2012 through January 2013, Boston agents and AUSA Stephen Heymann conduct witness preparation for the upcoming trial.

On January 11, 2013, Aaron Swartz committed suicide in Brooklyn, NY. The investigation is ongoing by New York City Police Department.

On February 6, 2013, a trial by jury in the U.S. District Court of Massachusetts was scheduled.

Case Agent: SA (b)(6),(b)(7)(C) (BOS)

Case Number: J-102-775-60071-S

## **HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Saturday, January 12, 2013 2:25 PM  
**To:** (b)(6),(b)(7)(C) (CID)  
**Cc:** HUGH DUNLEAVY (INV)  
**Subject:** Re: CID/CERT: Update for Case Support to Boston Field Office: Aaron Swartz Suicide Confirmed

Thx. Notification made to GPA earlier this morning. See following -

----- Original Message -----

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Saturday, January 12, 2013 09:54 AM Eastern Standard Time  
**To:** LEE FIELDS (INV); EDWIN DONOVAN (GPA)  
**Subject:** Fw: Aaron Swartz (USSS Defendant Commits Suicide - awaiting positive ME ID)

Lee and Ed:

I was advised of this situation this morning, there could be some media attention regarding our defendant committing suicide. This case was about to go to Federal trial.

Our investigation revealed that Swartz had hacked into MIT servers and obtained gigabytes of data primarily dealing with technical manuals.

Please confirm with me that you received this info.

Thanks - Steve

Steven D. Ricciardi  
Special Agent In Charge  
United States Secret Service  
Boston Field Office  
(617) 565-5640

----- Original Message -----

**From:** (b)(6),(b)(7)(C) (BOS)  
**Sent:** Saturday, January 12, 2013 09:29 AM Eastern Standard Time  
**To:** STEVEN RICCIARDI (BOS)  
**Subject:** Aaron Swartz

Steve.

Please call when you have a moment. We have information that the MIT defendant Aaron Swartz committed suicide last night. Blogs are confirming and the NYC ME is confirming they have a Aaron swartz. (b)(6),(b)(7)(C) is following up with NYC to ensure positive confirmation.

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

**USSS - ASAC**  
**Boston Field Office**  
**(b)(6),(b)(7)(C)**

**From:** (b)(6), (b)(7)(C) [redacted] CID)  
**Sent:** Saturday, January 12, 2013 02:21 PM Eastern Standard Time  
**To:** (b)(6), (b)(7)(C) CID)  
**Cc:** JONATHAN BARTLETT (CID); HUGH DUNLEAVY (INV); EDWIN DONOVAN (GPA)  
**Subject:** Re: CID/CERT: Update for Case Support to Boston Field Office: Aaron Swartz Suicide Confirmed

Thank you (b) (6) (b) (7)(C) I have copied the chain and GPA on this chain. Who is the case agent from Boston?

**From:** (b)(6), (b)(7)(C) (CID)  
**Sent:** Saturday, January 12, 2013 02:08 PM  
**To:** (b)(6), (b)(7)(C) (CID)  
**Subject:** CID/CERT: Update for Case Support to Boston Field Office: Aaron Swartz Suicide Confirmed

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

**We've been assisting the Boston Field Office in an investigation involving Aaron Swartz, the founder of Reddit, where he gained unauthorized access to MIT and stole data. Agents from the Boston Field Office arrested him while he was committing the crime.**

**It appears that he has committed suicide. Given that he is well known through his association with Reddit and Wired magazine I would not be surprised if there were to be media inquiries / coverage regarding his death.**

**R/**

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

**ATSAIC, Program Manager**  
**CID/CERT**  
**U.S. Secret Service**  
**(b)(6),(b)(7)(C) (Desk)**  
**(b)(6),(b)(7)(C) (Mobile)**  
**412-268-9262 (Fax)**

**From:** (b)(6),(b)(7)(C) [redacted]@cambridgepolice.org  
**Sent:** Saturday, January 12, 2013 10:32 AM Eastern Standard Time  
**To:** (b)(6),(b)(7)(C) [redacted] BOS; (b)(6),(b)(7)(C) [redacted] (BOS); (b)(6),(b)(7)(C) [redacted] (BOS); (b)(6),(b)(7)(C) [redacted] (BOS); (b)(6),(b)(7)(C) [redacted]  
(b)(6),(b)(7)(C) [redacted] (BOS); (b)(6),(b)(7)(C) [redacted] Gmail; (b)(6),(b)(7)(C) [redacted] @gmail.com> (b)(6),(b)(7)(C) [redacted] @gmail.com  
(b)(6),(b)(7)(C) [redacted] @gmail.com>  
**Cc:** (b)(6),(b)(7)(C) [redacted] @mit.edu; (b)(6),(b)(7)(C) [redacted] @MIT.EDU> (b)(6),(b)(7)(C) [redacted] MIT  
(b)(6),(b)(7)(C) [redacted] MIT.EDU> (b)(6),(b)(7)(C) [redacted] @mit.edu; (b)(6),(b)(7)(C) [redacted] @mit.edu> (b)(6),(b)(7)(C) [redacted] CID)  
**Subject:** Aaron Swartz Suicide Confirmed

**All Concerned,**

**This morning I was notified that Aaron Swartz committed suicide.**

**I have subsequently confirmed this report through The New York Medical Examiner's Office and NYPD's 71st Precinct Detectives.**

At 19:35 hours yesterday, January 11, 2013, the incident was reported to NYPD. Detective (b) of the 71 responded to (b)(6),(b)(7)(C) Aaron Swartz was identified and all indications thus far reveal that it is a suicide (b)(6),(b)(7)(C)

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

The New York Medical Examiner's Office has it listed as an open case at this time.

Detective (b)(6) will be calling me with further information. As I get more I shall pass it on.

R/S,

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

Detective  
Electronic Crimes Task Force  
USSS Boston Field Office  
10 Causeway Street (b)(6),(b)(7)(C)  
Boston, MA 02222

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

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

(b)(6),(b)(7)(C) [cambridgepolice.org](http://cambridgepolice.org)

## **HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Monday, January 14, 2013 10:16 AM  
**To:** JONATHAN BARTLETT (CID); invsp  
**Cc:** HUGH DUNLEAVY (INV)  
**Subject:** FW: MIT Case Boston  
**Attachments:** July 21, 2011.docx

**From:** (b)(6),(b)(7)(C) (INV)  
**Sent:** Monday, January 14, 2013 9:45 AM  
**To:** JANE MURPHY (INV); HUGH DUNLEAVY (INV); FREDERICK SELLERS (INV)  
**Cc:** (b)(6),(b)(7)(C) (INV); (b)(6),(b)(7)(C) (INV)  
**Subject:** MIT Case Boston

For Situational Awareness, attached is the write-up for the case involving MIT and the Defendant Aaron Swartz, who committed suicide over the weekend.

(b)(6),(b)(7)(C)  
*Special Agent*  
*United States Secret Service*  
*Office of Investigations / Special Projects*  
**Office:** (b)(6),(b)(7)(C)  
**Cell:** (b)(6),(b)(7)(C)

## **HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Tuesday, January 15, 2013 7:24 AM  
**To:** CYNTHIA TRIPLET (TEC); MARK COPANZZI (IRM)  
**Cc:** HUGH DUNLEAVY (INV); dadinv  
**Subject:** BOS MIT Investigation  
**Attachments:** July 21, 2011.docx

All,

FYSA – The USSS (BOS) was involved in the federal arrest and prosecution of defendant Aaron Swartz. Open source media reports hacker groups targeting MIT w/ retaliatory operations assumedly in response to defendant Swartz' suicide. (b)(5) (b)(5)

(b)(5)

Reference is made to the attached and following open source media web links:

- Anonymous Hacks MIT Sites To Post Aaron Swartz Tribute, Call To Arms (The Washington Post) - [http://www.washingtonpost.com/business/technology/anonymous-hacks-mit-sites-to-post-aaron-swartz-tribute-call-to-arms/2013/01/14/ff6f706c-5e44-11e2-9940-6fc488f3fecf\\_story.html?hpid=z10](http://www.washingtonpost.com/business/technology/anonymous-hacks-mit-sites-to-post-aaron-swartz-tribute-call-to-arms/2013/01/14/ff6f706c-5e44-11e2-9940-6fc488f3fecf_story.html?hpid=z10)
- [rememberaaronsw.tumblr.com/post/40372208044/official-statement-from-the-family-and-partner-of-aaron](http://rememberaaronsw.tumblr.com/post/40372208044/official-statement-from-the-family-and-partner-of-aaron)

Call w/ questions. V/r Hugh



## HUGH DUNLEAVY (VPD)

From: HUGH DUNLEAVY (INV)  
Sent: Tuesday, January 22, 2013 1:24 PM  
To: STEVEN RICCIARDI (BOS); (b)(6),(b)(7)(C) (BOS)  
Cc: HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID); dadinv  
Subject: FW: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-800710-8)

Gentlemen,

Reference the following. This congressional staff briefing will likely take place in the near future. I will represent the USSS. Please advise the assigned BOS AUSA and request the required 6e authority. In addition, BOS is requested to provide bulleted briefing points (separate from the case reports), organized by date, summarizing facts of USSS/ECTF and other LE specific involvement in this investigation.

i.e.:

- 26SEP2010 - MIT notified by JSTOR of .....
- 27SEP2010 - MIT identifies ip address xxx.xxxxx .....

The intent is to provide specific and factual USSS/LE investigation briefing and allow DOJ to speak to the associated judicial action (proffers, indictments, warrants, plea offers etc.)  
Call w/ questions. V/r Hugh

-----Original Message-----

From: FARON PARAMORE (GPA)  
Sent: Tuesday, January 22, 2013 1:05 PM  
To: PAUL MORRISSEY (GPA); JANE MURPHY (INV); HUGH DUNLEAVY (INV)  
Cc: FARON PARAMORE (GPA); LYNDIA WILLIAMS (GPA)  
Subject: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee

Good afternoon, hope you are well.

SAIC Williams and I just spoke with Ms. (b)(6),(b)(7)(C) from DOJ's Office of Legislative Affairs.

Ms. (b)(6),(b)(7)(C) advised that they were also telephonically contacted by Chairman Issa's staff last Thursday afternoon, requesting to provide a briefing on the Swartz case.

Consult with outside agency.

I will advise the group of DOJ's decision once I hear back from Ms. (b)(6),(b)(7)(C)

Thanks much.

Faron.

Faron K. Paramore

**Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service**

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

## **HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Tuesday, January 22, 2013 1:37 PM  
**To:** (b)(6),(b)(7)(C) (BOS)  
**Cc:** STEVEN RICCIARDI (BOS)  
**Subject:** Re: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

No date at this time.

----- Original Message -----

**From:** (b)(6),(b)(7)(C) (BOS)  
**Sent:** Tuesday, January 22, 2013 01:30 PM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** STEVEN RICCIARDI (BOS)  
**Subject:** RE: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Hugh,

We're on it. Do you have a date when you need the requested information?

Thanks,

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

Assistant Special Agent in Charge  
Boston Field Office

(b)(6),(b)(7)(C) Cell  
Office

-----Original Message-----

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Tuesday, January 22, 2013 1:24 PM  
**To:** STEVEN RICCIARDI (BOS); (b)(6),(b)(7)(C) (BOS)  
**Cc:** HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID); dadinv  
**Subject:** FW: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Gentlemen,

Reference the following. This congressional staff briefing will likely take place in the near future. I will represent the USSS. Please advise the assigned BOS AUSA and request the required 6e authority. In addition, BOS is requested to provide bulleted briefing points (separate from the case reports), organized by date, summarizing facts of USSS/ECTF and other LE specific involvement in this investigation.

i.e.:

- 26SEP2010 - MIT notified by JSTOR of .....
- 27SEP2010 - MIT identifies ip address xxx.xxxxx .....

The intent is to provide specific and factual USSS/LE investigation briefing and allow DOJ to speak to the associated judicial action (proffers, indictments, warrants, plea offers etc.)  
Call w/ questions. V/r Hugh

-----Original Message-----

From: FARON PARAMORE (GPA)

Sent: Tuesday, January 22, 2013 1:05 PM

To: PAUL MORRISSEY (GPA); JANE MURPHY (INV); HUGH DUNLEAVY (INV)

Cc: FARON PARAMORE (GPA); LYNDIA WILLIAMS (GPA)

Subject: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee

Good afternoon, hope you are well.

SAIC Williams and I just spoke with Ms. (b)(6),(b)(7)(C) from DOJ's Office of Legislative Affairs.

Ms. (b)(6),(b)(7)(C) advised that they were also telephonically contacted by Chairman Issa's staff last Thursday afternoon, requesting to provide a briefing on the Swartz case.

Consult with outside agency.

I will advise the group of DOJ's decision once I hear back from Ms. (b)(6),(b)(7)(C)

Thanks much.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
(b)(6),(b)(7)(C) Cell  
(202) 406-5740 Fax

## **HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 24, 2013 4:42 PM  
**To:** STEVEN RICCIARDI (BOS); JONATHAN BARTLETT (CID)  
**Cc:** HUGH DUNLEAVY (INV)  
**Subject:** See Attached - Note BOS SA named  
**Attachments:** Rolling Stone Magazine.23JAN2013.doc

Call w/ questions. V/r Hugh

**RIF**

337

**HUGH DUNLEAVY (VPD)**

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 24, 2013 6:14 PM  
**To:** CYNTHIA TRIPLETT (TEC); (b)(6), (b)(7)(C) (TEC); MARK COPANZZI (IRM)  
**Cc:** dadinv; HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID); (b)(6), (b)(7)(C) (CID); (b)(6), (b)(7)(C) (CID); (b)(6), (b)(7)(C) (CID)  
**Subject:** RE: BOS MIT Investigation  
**Attachments:** Rolling Stone Magazine.23JAN2013.doc  
**Importance:** High

**All,**

Reference previous and attached. The attached open source media specifically cites the USSS and the BOS SA involvement in this investigation. While there continue to be (b)(5)

**Call w/ questions. V/r Hugh**

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Tuesday, January 15, 2013 7:24 AM  
**To:** CYNTHIA TRIPLETT (TEC) (b)(6),(b)(7)(C) (TEC) (b)(6),(b)(7)(C) (IRM)  
**Cc:** HUGH DUNLEAVY (INV); dadinv  
**Subject:** BOS MIT Investigation

## All:

**FYSA – The USSS (BOS) was involved in the federal arrest and prosecution of defendant Aaron Swartz. Open source media reports hacker groups targeting MIT w/ retaliatory operations assumedly in response to defendant Swartz' suicide.** (b)(5)

**Reference is made to the attached and following open source media web links:**

- Anonymous Hacks MIT Sites To Post Aaron Swartz Tribute, Call To Arms (The Washington Post) - [http://www.washingtonpost.com/business/technology/anonymous-hacks-mit-sites-to-post-aaron-swartz-tribute-call-to-arms/2013/01/14/ff6f706c-5e44-11e2-9940-6fc488f3fecdd\\_story.html?hpid=hp\\_hp-top-table-main-swartz-tribute:homepage-link-story&hpid=hp\\_hp-top-table-main-swartz-tribute:homepage-link-story](http://www.washingtonpost.com/business/technology/anonymous-hacks-mit-sites-to-post-aaron-swartz-tribute-call-to-arms/2013/01/14/ff6f706c-5e44-11e2-9940-6fc488f3fecdd_story.html?hpid=hp_hp-top-table-main-swartz-tribute:homepage-link-story&hpid=hp_hp-top-table-main-swartz-tribute:homepage-link-story)
- [rememberaaronsw.tumblr.com/post/40372208044/official-statement-from-the-family-and-partner-of-aaron](http://rememberaaronsw.tumblr.com/post/40372208044/official-statement-from-the-family-and-partner-of-aaron)

**Call w/ questions. V/r Hugh**

## **HUGH DUNLEAVY (VPD)**

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 24, 2013 6:32 PM  
**To:** STEVEN RICCIARDI (BOS)  
**Cc:** HUGH DUNLEAVY (INV); (b)(6),(b)(7)(C) (BOS); JONATHAN BARTLETT (CID)  
**Subject:** RE: Call w/ DOJ regarding Aaron Swartz case / Briefing to House Oversight & Gov't Reform Committee (102-775-600710-S) - SUSPENSE NLT WED 30JAN2013

Gentlemen,

FYSA - Now appears to be FRI 01FEB2013 for the investigation briefing to House Oversight & Gov't Reform Committee. I will provide the USSS portion. Please plan to have the requested time line and bulleted briefing points by NLT WED 30JAN2013.

USSS GPA has been in contact w/ their DOJ equivalent. Please insure the BOS USAO is aware of the planned briefing, share w/ the USAO the time line and bulleted briefing points and request clearance for any potential 6e issues. The intent is for the USSS to brief investigative facts only. I will defer to DOJ to address any judicial action.

Call w/ questions. Thanks Hugh

-----Original Message-----

**From:** (b)(6),(b)(7)(C) (BOS)  
**Sent:** Tuesday, January 22, 2013 1:30 PM  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** STEVEN RICCIARDI (BOS)  
**Subject:** RE: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Hugh,

We're on it. Do you have a date when you need the requested information?

Thanks,

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

Assistant Special Agent in Charge  
Boston Field Office

(b)(6),(b)(7)(C) ell  
ffice

-----Original Message-----

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Tuesday, January 22, 2013 1:24 PM  
**To:** STEVEN RICCIARDI (BOS); (b)(6),(b)(7)(C) (BOS)  
**Cc:** HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID); dadinv  
**Subject:** FW: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Gentlemen,

Reference the following. This congressional staff briefing will likely take place in the near future. I will represent the USSS. Please advise the assigned BOS AUSA and request the required 6e authority. In addition, BOS is requested to provide bulleted briefing points (separate from the case reports), organized by date, summarizing facts of USSS/ECTF and other LE specific involvement in this investigation.

i.e.:

- 26SEP2010 - MIT notified by JSTOR of .....
- 27SEP2010 - MIT identifies ip address xxx.xxxxx .....

The intent is to provide specific and factual USSS/LE investigation briefing and allow DOJ to speak to the associated judicial action (proffers, indictments, warrants, plea offers etc.) Call w/ questions. V/r Hugh

-----Original Message-----

From: FARON PARAMORE (GPA)

Sent: Tuesday, January 22, 2013 1:05 PM

To: PAUL MORRISSEY (GPA); JANE MURPHY (INV); HUGH DUNLEAVY (INV)

Cc: FARON PARAMORE (GPA); LYNDIA WILLIAMS (GPA)

Subject: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee

Good afternoon, hope you are well.

SAIC Williams and I just spoke with Ms. (b)(6),(b)(7)(C) from DOJ's Office of Legislative Affairs.

Ms. (b)(6),(b) advised that they were also telephonically contacted by Chairman Issa's staff last Thursday afternoon, requesting to provide a briefing on the Swartz case.

Consult with outside agency.

I will advise the group of DOJ's decision once I hear back from Ms. (b)(6),(b)

Thanks much.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax



**HUGH DUNLEAVY (VPD)**

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 24, 2013 7:09 PM  
**To:** (b)(6),(b)(7)(C) (BOS)  
**Subject:** RE: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-5) - SUSPENSE NLT WED 30JAN2013

Thx (b)(6).

-----Original Message-----

**From:** (b)(6),(b)(7)(C) (BOS)  
**Sent:** Thursday, January 24, 2013 7:05 PM  
**To:** HUGH DUNLEAVY (INV); STEVEN RICCIARDI (BOS); (b)(6),(b)(7)(C) (BOS)  
**Cc:** JONATHAN BARTLETT (CID)  
**Subject:** Re: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-5) - SUSPENSE NLT WED 30JAN2013

Boston copies. We'll have the briefing point to you prior to the deadline.

Thanks.

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

USSS - ASATC  
Boston Field Office

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

----- Original Message -----

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 24, 2013 06:31 PM  
**To:** STEVEN RICCIARDI (BOS)  
**Cc:** HUGH DUNLEAVY (INV); (b)(6),(b)(7)(C) (BOS); JONATHAN BARTLETT (CID)  
**Subject:** RE: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-5) - SUSPENSE NLT WED 30JAN2013

Gentlemen,

FYSA - Now appears to be FRI 01FEB2013 for the investigation briefing to House Oversight & Gov't Reform Committee. I will provide the USSS portion.  
Please plan to have the requested time line and bulleted briefing points by NLT WED 30JAN2013.

USSS GPA has been in contact w/ their DOJ equivalent. Please insure the BOS USAO is aware of the planned briefing, share w/ the USAO the time line and bulleted briefing points and request clearance for any potential 6e issues. The intent is for the USSS to brief investigative facts only. I will defer to DOJ to address any judicial action.

Call w/ questions. Thanks Hugh

-----Original Message-----

**From:** (b)(6),(b)(7)(C) (BOS)  
**Sent:** Tuesday, January 22, 2013 1:30 PM  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** STEVEN RICCIARDI (BOS)

Subject: RE: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Hugh,

We're on it. Do you have a date when you need the requested information?

Thanks,

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

Assistant Special Agent in Charge  
Boston Field Office

(b)(6),(b)(7)(C) Cell  
Office

-----Original Message-----

From: HUGH DUNLEAVY (INV)

Sent: Tuesday, January 22, 2013 1:24 PM

To: STEVEN RICCIARDI (BOS); (b)(6),(b)(7)(C) (BOS)

Cc: HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID); dadinv

Subject: FW: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Gentlemen,

Reference the following. This congressional staff briefing will likely take place in the near future. I will represent the USSS. Please advise the assigned BOS AUSA and request the required 6e authority. In addition, BOS is requested to provide bulleted briefing points (separate from the case reports), organized by date, summarizing facts of USSS/ECTF and other LE specific involvement in this investigation.

i.e.:

- 26SEP2010 - MIT notified by JSTOR of .....
- 27SEP2010 - MIT identifies ip address xxx.xxxxx .....

The intent is to provide specific and factual USSS/LE investigation briefing and allow DOJ to speak to the associated judicial action (proffers, indictments, warrants, plea offers etc.)  
Call w/ questions. V/r Hugh

-----Original Message-----

From: FARON PARAMORE (GPA)

Sent: Tuesday, January 22, 2013 1:05 PM

To: PAUL MORRISSEY (GPA); JANE MURPHY (INV); HUGH DUNLEAVY (INV)

Cc: FARON PARAMORE (GPA); LYNDIA WILLIAMS (GPA)

Subject: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee

Good afternoon, hope you are well.

SAIC Williams and I just spoke with Ms (b)(6),(b)(7)(C) from DOJ's Office of Legislative Affairs.

Ms (b)(6),(b)(7)(C) advised that they were also telephonically contacted by Chairman Issa's staff last Thursday afternoon, requesting to provide a briefing on the Swartz case.

Consult with outside agency.

I will advise the group of DOJ's decision once I hear back from Ms. (b)(6),(b)(7)

Thanks much.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

**HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Friday, January 25, 2013 1:59 PM  
**To:** (b)(6),(b)(7)(C) (BOS)  
**Subject:** RE: FREEDOM OF INFORMATION ACT & PRIVACY ACT REQUEST FILE # 20130262

Recv'd - thanks Hugh

-----Original Message-----

**From:** (b)(6),(b)(7)(C) (BOS)  
**Sent:** Friday, January 25, 2013 1:49 PM  
**To:** (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)  
**Cc:** (b)(6),(b)(7)(C) (BOS); STEVEN RICCIARDI (BOS); HUGH DUNLEAVY (INV)  
**Subject:** FW: FREEDOM OF INFORMATION ACT & PRIVACY ACT REQUEST FILE # 20130262

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

Please respond to this message via official message:

"Secret Service Case Number J-102-775-0060071-S, in the name of Aaron Swartz is still an open case. The requested information will be copied and will be held in the Boston Field Office until said case is closed. At that time, the requested information will be forwarded to Liaison Division for disclosure as deemed appropriate. "

Thanks,

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

Assistant Special Agent in Charge  
Boston Field Office

(b)(6),(b)(7)(C) Cell  
Office

-----Original Message-----

**From:** BOS  
**Sent:** Friday, January 25, 2013 1:06 PM  
**To:** (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)  
**Cc:** (b)(6),(b)(7)(C) (BOS); STEVEN RICCIARDI (BOS); (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)  
**Subject:** FW: FREEDOM OF INFORMATION ACT & PRIVACY ACT REQUEST FILE # 20130262

Response due by Noon on Monday 1/28/13.

-----Original Message-----

**From:** lia  
**Sent:** Friday, January 25, 2013 11:49 AM  
**To:** BOS  
**Subject:** FREEDOM OF INFORMATION ACT & PRIVACY ACT REQUEST FILE # 20130262

//ROUTINE//

FM : FOIA/PA OFFICER, LIAISON DIVISION

FILE: 177.060/177.070

TO : BOSTON FIELD OFFICE

SUBJ : FREEDOM OF INFORMATION ACT & PRIVACY ACT REQUEST

REFERENCE IS MADE TO THE INVESTIGATIVE MANUAL, SECTIONS 48 & 49.

PLEASE CONDUCT A CHECK OF YOUR RECORDS, TO INCLUDE EMAILS AND HANDWRITTEN NOTES, FOR INFORMATION CONCERNING THE FOLLOWING [INDIVIDUAL(S)/ORGANIZATION(S)/EVENT(S)]. IF YOUR FILES SHOW THAT YOU WERE THE CONTROLLING FIELD OFFICE, PLEASE NOTIFY THE FOIA/PA OFFICE BY OFFICIAL MESSAGE BEFORE NOON THE FOLLOWING WORKING DAY STATING THAT DOCUMENTS HAVE BEEN LOCATED. PLEASE NOTE, EVEN IF RESULTS ARE NEGATIVE, PLEASE NOTIFY OUR OFFICE.

COPIES OF THE ENTIRE FILE SHOULD BE IMMEDIATELY SENT, VIA FEDERAL EXPRESS, TO THE FOIA/PA OFFICE. PLEASE ENSURE THAT THE ENTIRE FILE IS PHOTOCOPIED AND ALL COPIES ARE LEGIBLE. INCLUDE ALL REVERSE SIDES, STANDARD FORMS, PHOTOS, AND HANDWRITTEN NOTES.

IF THE FIELD OFFICE FILE IS OPEN OR IF DISCLOSURE OF INFORMATION IN A CLOSED FILE COULD ADVERSELY AFFECT A PENDING INVESTIGATION OR PROSECUTION, PLEASE CONTACT THE FOIA/PA OFFICE AT (202) 406-5838 BEFORE COPIES OF THE FILE ARE FORWARDED.

ANY DELAY IN FORWARDING RESPONSIVE DOCUMENTS SHOULD BE REPORTED TO THE FOIA/PA OFFICE.

NAME	DOB	SSN	CASE NO.
SWARTZ, AARON	11/08/1986	*** - ** - 0493	102-775-0060071-S

PLEASE INCLUDE THE FOIA/PA FILE NO. IN YOUR RESPONSE TO OUR OFFICE.

HEADQUARTERS/LIAISON DIVISION

(b)(6),(b) MILLS

## **HUGH DUNLEAVY (VPD)**

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Monday, January 28, 2013 10:37 AM  
**To:** STEVEN RICCIARDI (BOS)  
**Cc:** HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID)  
**Subject:** Fw: U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

**Importance:** High

Pls confirm

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Monday, January 28, 2013 09:31 AM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV); FREDERICK SELLERS (INV); JONATHAN BARTLETT (CID)  
**Cc:** PAUL MORRISSEY (GPA); FARON PARAMORE (GPA); LYNDIA WILLIAMS (GPA)  
**Subject:** U.S. Attorney's Office in Boston drop charges against Aaron Swartz. Please see article below. Can we have BFO confirm with AUSA's office

Good Morning everyone, hope you are well.

Please see article below.

Looks like the US Attorney's Office in Boston dropped the charges against Aaron Swartz. Can we please have the Boston Field Office confirm this information.

If - If this is correct / true, this would also nullify our concerns regarding 6E material - I think.

Thanks. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

## **Feds drop charges against late Internet activist Aaron Swartz**

Federal prosecutors in Boston have dropped charges against Internet activist Aaron Swartz after his death.

(Michael Francis McElroy / New York Times via Associated Press / January 30, 2009)  
By Jessica Gwynn

January 14, 2013, 10:38 a.m.

Federal prosecutors in Boston have dropped charges against Internet activist Aaron Swartz.

Swartz, 26, was found dead Friday in his New York apartment. He apparently had hanged himself.

Prosecutors filed the notice of dismissal on Monday.

Swartz's family blamed his death on "prosecutorial overreach."

The U.S. attorney's office could not be reached for comment.

Federal prosecutors alleged Swartz used MIT's computers to illegally access millions of academic articles through the JSTOR database, a subscription service for scholarly articles. He was indicted in 2011 and was scheduled to go to trial on 13 counts including computer fraud. Swartz faced the possibility of millions of dollars in fines and up to 35 years in prison.

The case was seen as a showdown pitting the government and commercial interests against Internet "freedom fighters."

MIT President L. Rafael Reif on Sunday appointed Hal Abelson, a professor of computer science and engineering and a founding director of Creative Commons and the Free Software Foundation, to "lead a thorough analysis of MIT's involvement."

As news spread over the weekend of Swartz's death, the Web collectively mourned for a brilliant young technologist and activist who wanted to set the world's information free yet could never escape his own demons.

Confided one friend: "I'm not surprised that this is how his life ended, and I bet many others feel the same way. So sad, he had so much potential and not enough joy in his life."

Swartz was just 14 when he helped create RSS, a tool that distributes online content. He was one of the founders of the social news site Reddit, which was bought by Conde Nast. But he was best known as an activist for free and open access to the world's information.

"Everything he did was aimed at world-changing and at activism," said friend and historian Rick Perlstein.

Now his death is being used to question government's aggressive criminal prosecution of Internet activists.

Anonymous allegedly hacked MIT's website and left a tribute for Swartz: "We do not consign blame or responsibility upon MIT for what has happened, but call for all those feel heavy-hearted in their proximity to this awful loss to acknowledge instead the responsibility they have — that we all have — to build and safeguard a future that would make Aaron proud."

## **HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Tuesday, January 29, 2013 4:59 PM  
**To:** dadinv; invap  
**Cc:** HUGH DUNLEAVY (INV)  
**Subject:** FW: Aaron Swartz Case INV Request  
**Attachments:** Swartz INV Brief 1-29-2013.pdf

---

**From:** JONATHAN BARTLETT (CID)  
**Sent:** Tuesday, January 29, 2013 4:06 PM  
**To:** HUGH DUNLEAVY (INV)  
**Subject:** FW: Aaron Swartz Case INV Request

---

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 29, 2013 4:04 PM  
**To:** JONATHAN BARTLETT (CID); EDWARD LOWERY (PID)  
**Subject:** FW: Aaron Swartz Case INV Request

---

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 29, 2013 3:23 PM  
**To:** (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)  
**Cc:** (b)(6),(b)(7)(C) (CID)  
**Subject:** Aaron Swartz Case INV Request

Good afternoon, Please see attachment.

Thank you,

SA (b)(6),(b)(7)(C)  
United States Secret Service  
Criminal Investigative Division  
(b)(6),(b)(7)(C) Direct  
(b)(6),(b)(7)(C) Mobile  
Email: (b)(6),(b)(7)(C) [uss.s.dhs.gov](mailto:(b)(6),(b)(7)(C)@uss.s.dhs.gov)

---

**From:** (b)(6),(b)(7)(C) (BOS)  
**Sent:** Tuesday, January 29, 2013 3:16 PM  
**To:** (b)(6),(b)(7)(C) (CID)  
**Subject:** RE: Aaron Swartz Case

Please see attached

---

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Wednesday, January 23, 2013 10:18 AM  
**To:** (b)(6),(b)(7)(C) (BOS)  
**Subject:** Aaron Swartz Case



Good morning, Can you please give me a call regarding the INV request that was sent to your office yesterday regarding the above case?

Thank you,

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

United States Secret Service  
Criminal Investigative Division

(b)(6), (b)(7)(C) - Direct  
- Mobile

Email: (b)(6), (b)(7)(C) [uss.s.dhs.gov](mailto:uss.s.dhs.gov)

**HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Monday, January 14, 2013 10:15 AM  
**To:** JONATHAN BARTLETT (CID); invsp  
**Cc:** HUGH DUNLEAVY (INV)  
**Subject:** FW: MIT Case Boston  
**Attachments:** July 21, 2011.docx

---

**From:** (b)(6),(b)(7)(C) (INV)  
**Sent:** Monday, January 14, 2013 9:45 AM  
**To:** JANE MURPHY (INV); HUGH DUNLEAVY (INV); FREDERICK SELLERS (INV)  
**Cc:** (b)(6),(b)(7)(C) (INV) (b)(6),(b)(7)(C) (INV)  
**Subject:** MIT Case Boston

For Situational Awareness, attached is the write-up for the case involving MIT and the Defendant Aaron Swartz, who committed suicide over the weekend.

(b)(6),(b)(7)(C)  
*Special Agent*  
*United States Secret Service*  
*Office of Investigations / Special Projects*  
*Office* (b)(6),(b)(7)(C)  
*Cell* (b)(6),(b)(7)(C)

# **Criminal Investigative Division**

## **Daily Report**

**July 21, 2011**

***The information contained  
in this document is  
law enforcement sensitive.  
Dissemination is prohibited  
unless specifically authorized by the  
United States Secret Service  
Office of Investigations.***



**Homeland  
Security**



**RIF**

## **FIELD ACTIVITIES:**

### **Boston Field Office**

### **New England Electronic Crimes Task Force**

#### **MIT Network Intrusion Results in Federal Indictment and Arrest**

On January 4, 2011, Massachusetts Institute of Technology (MIT) Police Department contacted the Boston Field Office and requested assistance from the New England Electronic Crimes Task Force (NEECTF) regarding an investigation into a network intrusion. The initial investigation identified Aaron Swartz as the primary suspect.

NEECTF agents determined that Aaron Swartz intruded into the MIT network without authorization. Swartz broke into a locked closet containing network components, connected his computer to the MIT computer network and downloaded documents from a not-for-profit archive of scientific journals and academic work, known as "JSTOR." Swartz avoided MIT's and JSTOR's electronic security and distributed a significant amount of JSTOR's archive through one or more file-sharing sites. Through investigative interviews and electronic forensic evidence, agents established that Swartz's un-authorized access impaired MIT computers, disabled servers, and deprived various JSTOR users from accessing research. Agents discovered JSTOR and MIT were unable to block Swartz's attacks, as Swartz continued his intrusions utilizing new methods for accessing JSTOR. Subsequently Swartz exploited MIT's computer system to steal over four million articles from JSTOR.

On July 19, 2011, Aaron Swartz was arrested and appeared in U.S. District Court, District of Massachusetts, charged with violations of Title 18, United States Code, Section 1343 (Wire Fraud), Section 1030a2 (Theft of Information From a Computer), Section 1030 a5B (Recklessly Damaging a Computer) and Section 2 (Aiding and Abetting). This case is continued pending further judicial action.

Case Agent: SA (b)(6),(b)(7)(C) (BOS)

Case Number: J-102-775-60071-S

## **HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Tuesday, January 15, 2013 7:24 AM  
**To:** CYNTHIA TRIPLET (TEC); (b)(6),(b)(7)(C) (TEC); MARK COPANZZI (IRM)  
**Cc:** HUGH DUNLEAVY (INV); dadinv  
**Subject:** BOS MIT Investigation  
**Attachments:** July 21, 2011.docx

All,

FYSA – The USSS (BOS) was involved in the federal arrest and prosecution of defendant Aaron Swartz. Open source media reports hacker groups targeting MIT w/ retaliatory operations assumedly in response to defendant Swartz' suicide. At this time, INV/CID has no criminal intelligence suggesting that USSS systems will be specifically targeted in response to defendant Swartz' suicide.

Reference is made to the attached and following open source media web links:

- Anonymous Hacks MIT Sites To Post Aaron Swartz Tribute, Call To Arms (The Washington Post) - [http://www.washingtonpost.com/business/technology/anonymous-hacks-mit-sites-to-post-aaron-swartz-tribute-call-to-arms/2013/01/14/ff6f706c-5e44-11e2-9940-6fc488f3fecf\\_story.html?hpid=z10](http://www.washingtonpost.com/business/technology/anonymous-hacks-mit-sites-to-post-aaron-swartz-tribute-call-to-arms/2013/01/14/ff6f706c-5e44-11e2-9940-6fc488f3fecf_story.html?hpid=z10)
- [rememberaaronsw.tumblr.com/post/40372208044/official-statement-from-the-family-and-partner-of-aaron](http://rememberaaronsw.tumblr.com/post/40372208044/official-statement-from-the-family-and-partner-of-aaron)

Call w/ questions. V/r Hugh

## **HUGH DUNLEAVY (VPD)**

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 31, 2013 11:29 AM  
**To:** (b)(6),(b)(7)(C)  
**Cc:** dadinv; DONNA CAHILL (LEG); HUGH DUNLEAVY (INV); FARON PARAMORE (GPA)  
**Subject:** J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopsis  
**Attachments:** Swartz INV Brief 1-29-2013.pdf  
**Importance:** High

b6 b7C  
Attached for OCC review is the BOS summary of the J-102-775-600710-S investigation.  
This summary was offered to the USAO BOS for review and was declined.

I am scheduled to appear before the House Oversight & Gov't Reform Committee (OGR) Chairman Issa Staff on Friday, February 1, 2013.

SAIC BOS advises that the synopsis contains only information available in the unsealed indictment of Suspect Swartz.  
Pending your review, GPA will likely push to its DOJ counterpart.

Call w/ questions. V/r Hugh

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Wednesday, January 30, 2013 9:53 AM  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** FREDERICK SELLERS (INV)  
**Subject:** Final Draft of INV Requested Swartz Investigation Synopsis

Sir:

Attached is the final draft of the Swartz investigation synopsis. If you have any questions feel free to contact me or  
ASAC (b)(6),(b)(7)(C) at (b)(6),(b)(7)(C)

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service  
Boston Field Office  
617/563-5640

## **HUGH DUNLEAVY (VPD)**

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 31, 2013 2:18 PM  
**To:** (b)(6),(b)(7)(C)  
**Subject:** Re: J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopsis

1430. Headed back from WH now

---

**From:** (b)(6),(b)(7)(C) (LEG)  
**Sent:** Thursday, January 31, 2013 02:04 PM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV)  
**Subject:** RE: J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopsis

Hugh,

When you are ready I can walk over to your office and go over the doc.

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 31, 2013 11:29 AM  
**To:** (b)(6),(b)(7)(C) (LEG)  
**Cc:** dadinv; DONNA CAHILL (LEG); HUGH DUNLEAVY (INV); FARON PARAMORE (GPA)  
**Subject:** J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopsis  
**Importance:** High

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

Attached for OCC review is the BOS summary of the J-102-775-600710-S investigation. This summary was offered to the USAO BOS for review and was declined.

I am scheduled to appear before the House Oversight & Gov't Reform Committee (OGR) Chairman Issa Staff on Friday, February 1, 2013.  
SAIC BOS advises that the synopsis contains only information available in the unsealed indictment of Suspect Swartz. Pending your review, GPA will likely push to its DOJ counterpart.

Call w/ questions. V/r Hugh

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Wednesday, January 30, 2013 9:53 AM  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** FREDERICK SELLERS (INV)  
**Subject:** Final Draft of INV Requested Swartz Investigation Synopsis

Sir:

Attached is the final draft of the Swartz investigation synopsis. If you have any questions feel free to contact me or ASAC (b)(6),(b)(7)(C) at 617/565-5640.

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service

**Boston Field Office**  
**617/565-5640**

**RIF**



## **HUGH DUNLEAVY (VPD)**

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 31, 2013 2:19 PM  
**To:** FARON PARAMORE (GPA)  
**Subject:** Re: J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopsis

Tried. Call cell (b)(6),(b)(7)(C)

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Thursday, January 31, 2013 01:32 PM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV)  
**Subject:** Re: J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopsis

Hugh - faron here. Can you. Talk now???

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

---

**From:** FARON PARAMORE (GPA)  
**Sent:** Thursday, January 31, 2013 12:34 PM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV)  
**Subject:** FW: J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopsis

Hugh - Faron here. Leaving HQ now going up to the Hill.  
Again, please call me on my cell. I'm open until about 1:10pm.

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

Thanks.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Thursday, January 31, 2013 11:29 AM  
**To:** (b)(6),(b)(7)(C) (LEG)  
**Cc:** dadinv; DONNA CAHILL (LEG); HUGH DUNLEAVY (INV); FARON PARAMORE (GPA)  
**Subject:** J-102-775-600710-S - Final Draft of INV Requested Swartz Investigation Synopsis  
**Importance:** High

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

Attached for OCC review is the BOS summary of the J-102-775-600710-S investigation.  
This summary was offered to the USAO BOS for review and was declined.

I am scheduled to appear before the House Oversight & Gov't Reform Committee (OGR) Chairman Issa Staff on Friday, February 1, 2013.

SAIC BOS advises that the synopsis contains only information available in the unsealed indictment of Suspect Swartz. Pending your review, GPA will likely push to its DOJ counterpart.

Call w/ questions. V/r Hugh

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Wednesday, January 30, 2013 9:53 AM  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** FREDERICK SELLERS (INV)  
**Subject:** Final Draft of INV Requested Swartz Investigation Synopsis

Sir:

Attached is the final draft of the Swartz investigation synopsis. If you have any questions feel free to contact me or ASAI (b)(6), (b)(7)(C) at 617/565-5640.

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service  
Boston Field Office  
617/565-5640

**HUGH DUNLEAVY (VPD)**

---

**From:** HUGH DUNLEAVY (INV)  
**Sent:** Friday, February 01, 2013 2:20 PM  
**To:** STEVEN RICCIARDI (BOS); (b)(6), (b)(7)(C) (BOS)  
**Cc:** dadinv; JONATHAN BARTLETT (CID); EDWARD LOWERY (PID); HUGH DUNLEAVY (INV); FARON PARAMORE (GPA)  
**Subject:** J-102-775-600710-S - Requested OGR staff briefing complete

All,

The requested briefing to the House Oversight & Gov't Reform Committee (OGR) Chairman Issa's Staff was re. the BOS NEECTF investigation (J-102-775-600710-S) was completed by 1345 today.

Note - DOJ declined to attend.

No issues noted, No follow up or release of information requested, no indicated concern w/ the USSS investigation.

Thx to BOS and NEECTF for the support. The BOS investigation withstood scrutiny on its own merits and on the solid investigations and work of the NEECTF - well done.

Call w/ questions. V/r Hugh

---

**From:** STEVEN RICCIARDI (BOS)  
**Sent:** Wednesday, January 30, 2013 09:53 AM Eastern Standard Time  
**To:** HUGH DUNLEAVY (INV)  
**Cc:** FREDERICK SELLERS (INV)  
**Subject:** Final Draft of INV Requested Swartz Investigation Synopsis

Sir:

Attached is the final draft of the Swartz investigation synopsis. If you have any questions feel free to contact me or ASAIC (b)(6), (b)(7) at (b)(6), (b)(7)(C)

Steven D. Ricciardi  
Special Agent in Charge  
United States Secret Service  
Boston Field Office  
617/565-5640

## **HUGH DUNLEAVY (VPD)**

**Subject:** DOJ Briefing: J-102-775-80071-S  
**Location:** DOJ - 950 Pennsylvania Avenue, NW, (Visitor's Entrance on Constitution Avenue between 9th and 10th St., NW) - Office of Legislative Affairs - Suite 1145  
**Start:** Mon 2/11/2013 11:00 AM  
**End:** Mon 2/11/2013 12:00 PM  
**Show Time As:** Tentative  
**Recurrence:** (none)  
**Meeting Status:** Not yet responded  
**Organizer:** HUGH DUNLEAVY (INV)  
**Required Attendees:** FARON PARAMORE (GPA)

Hugh – we are all set for the meeting with DOJ next Monday, February 11<sup>th</sup> at 11 am. See below.

I'll send you a meeting request shortly.

Thanks. Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line  
(b)(6),(b)(7)(C) Direct line  
Cell  
(202) 406-5740 Fax

From: (b)(6),(b)(7)(C) (OLA) [mailto:(b)(6),(b)(7)(C)]@usdoj.gov  
Sent: Wednesday, February 06, 2013 2:51 PM  
To: FARON PARAMORE (GPA)  
Subject: Monday, 2/11/13 at 11:00 am

Consult with outside  
agency.

(b)

(b)(6),(b)(7)(C)  
Attorney Advisor  
Office of Legislative Affairs  
U.S. Department of Justice  
(b)(6),(b)(7)(C)



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

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 22, 2013 4:05 PM  
**To:** (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)  
**Cc:** (CID)  
**Subject:** Re: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

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

Let's discuss this tomorrow when we all return.

Thank you,

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

----- Original Message -----

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 22, 2013 03:47 PM Eastern Standard Time  
**To:** (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)  
**Cc:** (b)(6),(b)(7)(C) (CID)  
**Subject:** RE: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Sir,

We did provide the above summary for the SAIC regarding this case. Reference the attachment above. Just so I'm following in reference to the below...BOS is requested to provide bulleted briefing points (separate from the case reports) and will send to Regions and then ultimately to SP?

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

----- Original Message -----

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 22, 2013 2:14 PM  
**To:** JONATHAN BARTLETT (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)  
**Subject:** Re: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Copy

----- Original Message -----

**From:** JONATHAN BARTLETT (CID)  
**Sent:** Tuesday, January 22, 2013 02:11 PM Eastern Standard Time  
**To:** (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)  
**Subject:** RE: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Coordinate with BOS.

-----Original Message-----

From: (b)(6), (b)(7)(C) (CID)

Sent: Tuesday, January 22, 2013 2:05 PM

To: JONATHAN BARTLETT (CID); (b)(6), (b)(7)(C) (ID)

Subject: Re: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Special Projects have a ongoing briefing.

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

Can you ensure that the briefing is provided to the SAIC?

B

----- Original Message -----

From: JONATHAN BARTLETT (CID)

Sent: Tuesday, January 22, 2013 01:25 PM Eastern Standard Time

To: (b)(6), (b)(7)(C) (CID)

Subject: Fw: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

The Regions are working on bullet points for INV correct ?

SAIC Mark Bartlett

U.S. Secret Service

Criminal Investigative Division

----- Original Message -----

From: HUGH DUNLEAVY (INV)

Sent: Tuesday, January 22, 2013 01:23 PM Eastern Standard Time

To: STEVEN RICCIARDI (BOS); (b)(6), (b)(7)(C) (BOS)

Cc: HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID); dadinv

Subject: FW: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Gentlemen,

Reference the following. This congressional staff briefing will likely take place in the near future. I will represent the USSS. Please advise the assigned BOS AUSA and request the required 6e authority. In addition, BOS is requested to provide bulleted briefing points (separate from the case reports), organized by date, summarizing facts of USSS/ECTF and other LE specific involvement in this investigation.

I.e.:

- 26SEP2010 - MIT notified by JSTOR of .....
- 27SEP2010 - MIT identifies IP address xxx.xxxx .....

The intent is to provide specific and factual USSS/LE investigation briefing and allow DOJ to speak to the associated judicial action (proffers, indictments, warrants, plea offers etc.) Call w/ questions. V/r Hugh

-----Original Message-----

From: FARON PARAMORE (GPA)

Sent: Tuesday, January 22, 2013 1:05 PM

To: PAUL MORRISSEY (GPA); JANE MURPHY (INV); HUGH DUNLEAVY (INV)

Cc: FARON PARAMORE (GPA); LYNDA WILLIAMS (GPA)

Subject: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee

Good afternoon, hope you are well.

SAIC Williams and I just spoke with Ms. (b)(6),(b)(7)(C) from DOJ's Office of Legislative Affairs.

M (b)(6),(b)(7)(C) advised that they were also telephonically contacted by Chairman Issa's staff last Thursday afternoon, requesting to provide a briefing on the Swartz case.

Consult with outside agency.

I will advise the group of DOJ's decision once I hear back from Ms (b)(6),

Thanks much.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line

(b)(6),(b)(7)(C) Direct line

Cell

(202) 406-5740 Fax



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

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 22, 2013 3:48 PM  
**To:** (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)  
**Cc:** (b)(6),(b)(7)(C) (CID)  
**Subject:** RE: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)  
**Attachments:** FW: MIT Case Update

Sir,

We did provide the above summary for the SAIC regarding this case. Reference the attachment above. Just so I'm following in reference to the below...BOS is requested to provide bulleted briefing points (separate from the case reports) and will send to Regions and then ultimately to SP?

(b)(6),

-----Original Message-----

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 22, 2013 2:14 PM  
**To:** JONATHAN BARTLETT (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)  
**Subject:** Re: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Copy

----- Original Message -----

**From:** JONATHAN BARTLETT (CID)  
**Sent:** Tuesday, January 22, 2013 02:11 PM Eastern Standard Time  
**To:** (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)  
**Subject:** RE: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Coordinate with BOS.

-----Original Message-----

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Tuesday, January 22, 2013 2:05 PM  
**To:** JONATHAN BARTLETT (CID); (b)(6),(b)(7)(C) (CID)  
**Subject:** Re: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Special Projects have a ongoing briefing.

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

Can you ensure that the briefing is provided to the SAIC?

B.

----- Original Message -----

From: JONATHAN BARTLETT (CID)

Sent: Tuesday, January 22, 2013 01:25 PM Eastern Standard Time

To: (b)(6), (b)(7)(C) (CID)

Subject: Fw: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

The Regions are working on bullet points for INV correct ?

SAIC Mark Bartlett

U.S. Secret Service

Criminal Investigative Division

----- Original Message -----

From: HUGH DUNLEAVY (INV)

Sent: Tuesday, January 22, 2013 01:23 PM Eastern Standard Time

To: STEVEN RICCIARDI (BOS) (b)(6), (b)(7)(C) (BOS)

Cc: HUGH DUNLEAVY (INV); JONATHAN BARTLETT (CID); dadinv

Subject: FW: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee (102-775-600710-S)

Gentlemen,

Reference the following. This congressional staff briefing will likely take place in the near future. I will represent the USSS. Please advise the assigned BOS AUSA and request the required 6e authority. In addition, BOS is requested to provide bulleted briefing points (separate from the case reports), organized by date, summarizing facts of USSS/ECTF and other LE specific involvement in this investigation.

I.e.:

- 26SEP2010 - MIT notified by JSTOR of .....
- 27SEP2010 - MIT identifies ip address xxx.xxx.xx .....

The intent is to provide specific and factual USSS/LE investigation briefing and allow DOJ to speak to the associated judicial action (proffers, indictments, warrants, plea offers etc.) Call w/ questions. V/r Hugh

-----Original Message-----

From: FARON PARAMORE (GPA)

Sent: Tuesday, January 22, 2013 1:05 PM

To: PAUL MORRISSEY (GPA); JANE MURPHY (INV); HUGH DUNLEAVY (INV)

Cc: FARON PARAMORE (GPA); LYNDIA WILLIAMS (GPA)

Subject: Call w/ DOJ regarding Aaron Swartz case / briefing to House Oversight & Gov't Reform Committee

Good afternoon, hope you are well.

SAIC Williams and I just spoke with Ms (b)(6), (b)(7) from DOJ's Office of Legislative Affairs.

Ms (b)(6), advised that they were also telephonically contacted by Chairman Issa's staff last Thursday afternoon, requesting to provide a briefing on the Swartz case.

Consult with outside agency.

I will advise the group of DOJ's decision once I hear back from Ms. (b)(6), (b)(7)(C)

Thanks much.

Faron.

Faron K. Paramore  
Deputy Assistant Director  
Office of Congressional Affairs  
United States Secret Service

Ph: (202) 406-5676 Main line

(b)(6), (b)(7)(C) Direct line  
Cell

(202) 406-5740 Fax

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

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Monday, January 14, 2013 12:24 PM  
**To:** JONATHAN BARTLETT (CID)  
**Cc:** HUGH DUNLEAVY (INV)  
**Subject:** FW: MIT Case Update  
**Attachments:** MIT Case Update.docx

Sir,

Reference the above for an updated synopsis regarding case # J-102-775-60071-S (BOS). Further, for situational awareness purposes based on discussion with the case SA according to the NYPD Detective via the Boston PD Detective this incident was clearly a suicide. According to case SA (b)(6),(b)(7)(C) stated the subject suffered from a history of depression issues.

Regards,

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

**From:** (b)(6),(b)(7)(C) (CID)  
**Sent:** Monday, January 14, 2013 12:01 PM  
**To:** (b)(6),(b)(7)(C) (INV) (b)(6),(b)(7)(C) (INV) (b)(6),(b)(7)(C) (INV)  
**Cc:** CID.SP  
**Subject:** MIT Case Update

See updates on the MIT investigation.

(b)(6),(b)(7)(C)  
Special Agent  
Criminal Investigative Division / Special Projects  
Office: (b)(6),(b)(7)(C)  
Cell: (b)(6),(b)(7)(C)

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

From: BOS  
 Sent: Friday, January 21, 2011 2:59 PM  
 To: CID  
 Cc: ISD; BOS  
 Subject: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

## U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE FILE: 102-775-60071-S  
 TO: CRIMINAL INVESTIGATIVE DIVISION X-REF: N/A  
 INFO: INVESTIGATIVE SUPPORT DIVISION SEIZURE#: N/A  
 SUBJECT: OPENING REPORT

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)  
 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)(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)(7)(C) and Detective (b)(6),(b)(7)(C) of the Boston Police Department, traveled to MIT and met with (b)(6),(b)(7)(C) of the

1/27/2011

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

On 01/04/11, (b)(6),(b)(7)(C) emailed (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) and Infrastructure Services for MIT, asking them to further pinpoint the location of the computer downloading the journals. At 0808, (b)(6),(b)(7)(C) 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)(7)(C) established a packet capture of the same switch the computer was found attached to.

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

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)(C) of the MIT Police Department called (b)(6),(b)(7)(C) 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)(C) and SA (b)(6),(b)(7)(C) responded to Lee Street to assist (b)(6),(b)(7)(C). (b)(6),(b)(7)(C) attempted to interview Swartz, however Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) 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)(7)(C) 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) traced ghost-laptop on the network to building W20 on the 5th floor. MIT Building W20 is the Stratton Student Center. (b)(6),(b)(7)(C) 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)(7)(C) contacted (b)(6),(b)(7)(C) to inform him that they had traced the netbook to a room in the student center. SA (b)(6),(b)(7)(C) met (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) 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)(7)(C) 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)(7)(C) and (b)(6),(b)(7)(C) traveled to Cambridge Police Headquarters to interview Swartz. At Cambridge Headquarters, SA (b)(6),(b)(7)(C) met (b)(6),(b)(7)(C) 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)(C) AUSA Heymann and (b)(6),(b)(7)(C) from JSTOR conducted a conference call to discuss the theft of material from JSTOR.

1/27/2011

On 01/14/11, SA (b)(6),(b)(7)(C) Detective (b)(6), (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)(7)(C) 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 1152CR0079.

# SUSPECTS / DEFENDANTS:

SWARTZ, Aaron H. - SUSPECT

AKA: N/A  
 RACE: White  
 SEX: Male  
 DOB: 11/08/1986  
 SSN: (b)(6),(b)(7)(C)-1374  
 FBI: 675304KD0  
 SID: MA10556559  
 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/PLETS: 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.

1/27/2011

USSS / BOSTON

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

/ RICCIARDI

1/27/2011



Stephen Heymann held a conference call. (b)(6),(b)(7)(C) 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)(7)(C) 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)(7)(C) estimated that the value of the documents Swartz downloaded to be in excess of \$2 million. (b)(6),(b)(7)(C) stated that he believed the average cost of the articles was \$14.00. (b)(6),(b)(7)(C) stated that the first indication of an intrusion was a degradation of service for all customers. (b)(6),(b)(7)(C) 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)(7)(C) stated multiple download requests occurred simultaneously and that at times, hundreds of download requests were occurring concurrently. (b)(6),(b)(7)(C) confirmed that the JSTOR terms and conditions clearly prohibited the kind of downloading Swartz was doing.

On 02/03/11, SA (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) 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)(7)(C) and Detective (b)(6),(b)(7)(C) 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)(7)(C) and Detective (b)(6),(b)(7)(C) of the Cambridge Police, (b)(6),(b)(7)(C) from the Massachusetts Institute of Technology, and AUSA Stephen Heymann held a conference call. (b)(6),(b)(7)(C) 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)(7)(C) explained that previously (b)(6),(b)(7)(C) had sent an email to (b)(6),(b)(7)(C) describing the switch he had traced the excessive downloading from JSTOR to. (b)(6),(b)(7)(C) explained that after (b)(6),(b)(7)(C) found the laptop connected to the switch, he started a packet capture on the same switch. (b)(6),(b)(7)(C) 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)(7)(C) 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)(7)(C) said that he reviewed the packet capture and discovered 14 different IP addresses sending SSH traffic to the laptop. (b)(6),(b)(7)(C) believed that some of the IP addresses were SSH background noise, however he did note that (b)(6),(b)(7)(C) 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)(C) 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)(C) 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)(C) 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)(7)(C) stated that Swartz downloaded over 2.8 million documents in November and December of 2010. (b)(6),(b)(7)(C) 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 and 9,472 editorials.

On 02/11/11, SA (b)(6),(b)(7)(C) ATSAIC (b)(6),(b)(7)(C) SA (b)(6),(b)(7)(C) SA (b)(6),(b)(7)(C) and

3/2/2011

Detective (b)(6),(b)(7)(C) executed a federal search warrant on Swartz's residence located at (b)(6),(b)(7)(C). (b)(6),(b)(7)(C) Swartz was home at the time the search was executed. While the search was conducted, Swartz made statements to the effect of, what took you so long, and why didn't you do this earlier? The search team seized several items described in greater detail in the Evidence section of this report. After completing the search of Apartment 320, the search team returned to the first floor to search the storage locker allocated to apartment 320. While on the first floor, SA (b)(6),(b)(7)(C) observed Swartz leave the building, walk to the street and sprint away after he reached the street. After ascertaining that none of the items in the storage locker belonged to Swartz, the search team moved to (b)(6),(b)(7)(C) in (b)(6),(b)(7)(C) where the Harvard University, Edmond J. Safra Center for Ethics is located and Swartz is listed as a lab fellow. The search team observed Swartz at the Safra Center for Ethics. Harvard University Police secured Swartz's office while a federal search warrant was obtained. After the search warrant was obtained, the team searched Swartz's office at the Safra Center. SA (b)(6),(b)(7)(C) seized an Apple iMac computer and a Western Digital hard drive from Swartz's office.

On 02/25/11, Detective (b)(6),(b)(7)(C) received the Acer Aspire netbook, hard drive enclosure, Western Digital hard drive contained in the enclosure, and the USB flash drive from Cambridge Police Property Technician (b)(6),(b)(7)(C). Detective (b)(6),(b)(7)(C) took the evidence items directly to the ECSAP Lab Evidence Vault.

#### SUSPECTS/DEFENDANTS:

SWARTZ, Aaron H - SUSPECT

1599: Yes  
1599A: No

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

- SUBJECT

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

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

- SUBJECT

RACE: N/A  
SEX: (b)(6),(b)(7)(C)  
DOB:  
SSN:  
FBI: N/A  
SID: N/A  
HT: N/A  
WT: N/A

3/2/2011

EYES: (b)(6),(b)(7)(C)  
 HAIR: (b)(6),(b)(7)(C)  
 1599: No  
 1599A: No  
 PHOTO: No  
 PRINTS: No  
 POB:  
 DL/STATE:  
 ADDRESS: (b)(6),(b)(7)(C)  
 EMAIL:  
 DATABASE CHECKS: 02/24/11

## EXAMS CONDUCTED:

ECSAP: Ongoing  
 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:

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 31  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA (b)(6),(b)(7)(C)  
**DESCRIPTION OF ITEMS:** Scientific Atlantic Modem SN# SM1565969  
 Apple Multi Adapter SN# 6F9395N72U6  
 Apple Multi Adapter SN# 6F7281NNU48  
 Black Notebook Journal  
**SEIZED / OBTAINED FROM:** Aaron Swartz  
**LOCATION:** Boston Field Office Evidence Vault  
**DISPOSITION:** Held pending judicial action.

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 32  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA (b)(6),(b)(7)(C)  
**DESCRIPTION OF ITEMS:** Harvard University Earning Statement  
 Earning Statement Addressed to Aaron Swartz  
 Master's Thesis M-876 Lind  
 Western Digital Mail-in Rebate Form  
**SEIZED / OBTAINED FROM:** Aaron Swartz  
**LOCATION:** Boston Field Office Evidence Vault  
**DISPOSITION:** Held pending judicial action.

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 33  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA (b)(6),(b)(7)(C)  
**DESCRIPTION OF ITEMS:** Wireless-G 2.4 GHz Broadband Router Linksys  
 MacBook Mac OSX Install Disc one and two  
 MacBook User Guide in Gray Cardboard case  
 Apple Care Service Letter Dispatch R6276408  
 Genius Bar Work Confirmation  
**SEIZED / OBTAINED FROM:** Aaron Swartz  
**LOCATION:** Boston Field Office Evidence Vault

3/2/2011

**DISPOSITION:** Held pending judicial action.

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 34  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA (b)(6)(b)  
**DESCRIPTION OF ITEMS:** Nokia Cell Phone  
T-Mobile, HTC G2 cell phone  
12 Magnetic Media Tapes

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

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 35  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA (b)(6)(b)  
**DESCRIPTION OF ITEMS:** Metallic Blue iPod  
White iPod with carrying case  
White iPod with serial number SA6330856UX8A  
White iTalk  
Black 16GB Thumb-drive

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

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 36  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA (b)(6)(b)  
**DESCRIPTION OF ITEMS:** Fifty-four miscellaneous compact discs  
Two hard drive enclosures  
T-Mobile Sidekick  
Sony Micro Vault

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

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 37  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA (b)(6)(b)  
**DESCRIPTION OF ITEMS:** DVD-R with handwritten label  
Pocket notebook  
Pure Drive Quick start guide  
Disk utility internal hard drive upgrade kit  
Seagate Barracuda Hard Drive Installation Guide

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

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 38  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA (b)(6)(b)  
**DESCRIPTION OF ITEMS:** Apple iMac Model A1311 serial number WB025AXGD87  
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 LUSAX0D0010011001E1601

3/2/2011

SEIZED / OBTAINED FROM:  
LOCATION:  
DISPOSITION:

Rocketfish Enclosure with WD hard drive WMAZA1636675  
HP USB Drive marked 00458NKB71 85102  
Cambridge Police  
Boston Field Office Evidence Vault  
Held pending judicial action.

**DISPOSITION:**

The San Francisco Field Office is requested to interview (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) 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)(7) and (b)(6),(b)(7) the San Francisco agent assigned this IOD is requested to contact Boston case agent (b)(6),(b)(7)(C) 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

3/2/2011

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

(CID)

From:  
Sent:  
To:  
Cc:  
Subject:

SFO  
Thursday, June 23, 2011 4:38 PM  
CID: BOS  
ISD: SFO  
CT 775.510 (102-775-60071-S) REPORT OF IOD - AARON SWARTZ (CLOSED)

ORIGINAL

IOD

//ROUTINE//

U.S. SECRET SERVICE INVESTIGATIVE REPORT

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

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

SUBJECT: REPORT OF IOD

ACTUAL LOSS: \$TED

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)  
DATE CASE OPENED: 02/28/11 (b)(6),(b)(7)(C)  
PREVIOUS REPORT: N/A  
REPORTING PERIOD: 02/28/11 - 06/28/11  
STATUS: CLOSED

SYNOPSIS:

The Boston Field Office requested the San Francisco Field Office (SFO) to interview (b)(6), (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) two known associates of Aaron Swartz to determine their knowledge of his activities. After a discussion with Assistant United States Attorney (AUSA) Stephen Heymann, District of Massachusetts and case agent (b)(6),(b)(7)(C) (BOS), it was decided that the interview of (b)(6),(b)(7)(C) was not necessary. (b)(6),(b)(7)(C) was interviewed regarding her knowledge of Aaron Swartz's recent activities. Case closed in San Francisco.

DETAILS OF INVESTIGATION:

On 3/1/11, I participated in a conference call with SA (b)(6),(b)(7)(C) of the Boston Field Office (BOS) and AUSA Stephen Heymann. During this conversation, SA (b)(6),(b)(7)(C) and SA Heymann requested that I interview (b)(6),(b)(7)(C) first, and a decision on whether to interview (b)(6),(b)(7)(C) would be made at a later date. On 3/9/11, I responded to (b)(6),(b)(7)(C) residence. At this time, SA (b)(6),(b)(7)(C) and I interviewed (b)(6),(b)(7)(C) with (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C).

stated that she received a phone call from Swartz, who asked her to call his lawyer and arrange bail for him, which she did. (b)(6)(b)(7)(C)

(b)(6)(b)(7)(C) When (b)(6)(b)(7)(C) was asked about any additional contact with Swartz, 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 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)(7)(C) was asked if Swartz ever mentioned JSTOR records to her, and (b)(6)(b)(7)(C) 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)(7)(C) regarding the interview of (b)(6)(b)(7)(C). SA (b)(6)(b)(7)(C) advised he was preparing to indict Aaron Swartz and will consult with AUSA Heymann to determine if an interview with (b)(6)(b)(7)(C) is necessary.

On 6/10/11, I was contacted by SA (b)(6)(b)(7)(C) who advised that after a discussion with AUSA Heymann the interview of (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)(7)(C)

##### - SUBJECT

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

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

##### SUBJECT

AKA: N/A  
RACE: White

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

**EXAMS CONDUCTED:**

None.

**DATABASE SEARCHES CONDUCTED:**

None

**EVIDENCE / CONTRABAND / PERSONAL PROPERTY:**

None

**DISPOSITION:**

Case closed in San Francisco.

USSS/SAN FRANCISCO/jd

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

/MITCHELL



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

ORIGINAL

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  
SUBJECT: REPORT OF CONTINUING INVESTIGATION

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

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)  
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)(7)(C) on 02/28/11.

Reference is made to the Report of Investigation Other District written by SA (b)(6),(b)(7)(C) 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)(C) 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)(7)(C) AUSA Heymann, Detective (b)(6),(b)(7)(C) 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)(7)(C) AUSA Heymann, and (b)(6),(b)(7)(C) from JSTOR on 06/25/11.

On 03/09/11, SA (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) of the San Francisco Field Office interviewed (b)(6),(b)(7)(C)

The details of the interview are described in a Memorandum of Interview written by SA (b)(6),(b)(7)(C). A copy of that NOI will be maintained in this case folder.

On 04/13/11, SA (b)(6),(b)(7)(C), Detective (b)(6),(b)(7)(C) and AUSA Heymann, interviewed (b)(6),(b)(7)(C) at the U.S. Attorney's office at 1 Courthouse Way, Boston, Massachusetts. Also present were (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) both attorneys with Fish and Richardson. The details of the interview are described in a Memorandum of Interview written by SA (b)(6),(b)(7)(C). A copy of that NOI will be maintained in this case folder.

On 05/12/11, SA (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) interviewed (b)(6),(b)(7)(C) at the (b)(6),(b)(7)(C) Boston Massachusetts. The details of the interview are described in a Memorandum of Interview written by Detective (b)(6),(b)(7)(C). A copy of the NOI will be maintained in this case folder.

On 06/07/11, 4 Samsung Hard Drives were turned over to SA (b)(6),(b)(7)(C) at the offices of Good and Cormier located at 83 Atlantic Avenue in Boston Massachusetts.

**SUSPECTS / DEFENDANTS:**

SWARTZ, Aaron H. - SUSPECT

1599: Yes

1599A: No

(b)(6),(b)(7)(C) - SUBJECT

1599: No

1599A: No

(b)(6),(b)(7)(C) - SUBJECT

1599: No

1599A: No

**EXAMS CONDUCTED:**

RCSAP: Ongoing

Poly: N/A

FSD: N/A

**DATABASE SEARCHES CONDUCTED:**

NCI / CI: 01/07/11

NCIC/ULETS: 01/07/11

CCS/CPT: 01/07/11

LOCAL LE: 01/07/11

**EVIDENCE / CONTRABAND / PERSONAL PROPERTY:**

EVIDENCE SSF 1544 S/N:

DATE OF INVENTORY:

INVENTORY MADE BY:

DESCRIPTION OF ITEMS:

SEIZED / OBTAINED FROM:

LOCATION:

DISPOSITION:

102 2011 CE 81

02/25/11

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

16 CD contained in a mailing envelope

Aaron Swartz

Boston Field Office Evidence Vault

Held pending judicial action.

EVIDENCE SSF 1544 S/N:

102 2011 CE 82

DATE OF INVENTORY: 02/25/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)  
DESCRIPTION OF ITEMS: Galaxy Metal Gear Box External Hard Drive  
SEIZED / OBTAINED FROM: Aaron Swartz  
LOCATION: Boston Field Office Evidence Vault  
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/W: 102 2011 CB 119  
DATE OF INVENTORY: 06/07/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)  
DESCRIPTION OF ITEMS: 4 Samsung Hard Drives  
SEIZED / OBTAINED FROM: Aaron Swartz  
LOCATION: Boston Field Office ECSAP Vault  
DISPOSITION: Held pending judicial action.

All other evidence remains in the Boston Field Office Evidence vault as previously reported.

**DISPOSITION:**

Case continued pending further investigation and judicial action.

USSS / BOSTON

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

ORIGINAL

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

From: BOS  
Sent: Monday, August 01, 2011 1:38 PM  
To: CID  
Cc: ISD; BOS  
Subject: 775.510 Notification of Federal Arrest - Aaron Swartz (J-102-775-60071-S)

**U.S. SECRET SERVICE INVESTIGATIVE REPORT**

FROM: BOSTON FIELD OFFICE FILE: J-102-775-60071-S  
TO: CRIMINAL INVESTIGATIVE DIVISION X-REF: N/A  
INFO: INVESTIGATIVE SUPPORT DIVISION SEIZURE#: N/A

SUBJECT: NOTIFICATION OF FEDERAL ARREST  
AARON SWARTZ - Date of Arrest: 07/19/11

ACTUAL LOSS: \$TBD POTENTIAL LOSS: \$2,000,000.00

**FEDERAL STATUTES VIOLATED - TITLE 18 UNITED STATES CODE**

SECTION 1343 - WIRE FRAUD  
SECTION 1030(a)(4) - COMPUTER FRAUD  
SECTION 1030(a)(2) - THEFT OF INFORMATION FROM A COMPUTER  
SECTION 1030(a)(5)(B) - RECKLESSLY DAMAGING A COMPUTER  
SECTION 2 - AIDING AND ABETTING

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)  
DATE CASE OPENED: 01/07/11  
PREVIOUS REPORT: 06/29/11 - REPORT OF CONTINUING INVESTIGATION  
REPORTING PERIOD: 06/30/11 - 08/01/11  
STATUS: CONTINUED

**SYNOPSIS:**

Aaron Swartz was indicted in U.S. District Court for the District of Massachusetts for violations of Title 18 United States Code, Sections 1343 - Wire Fraud; 1030(a)(4) - Computer Fraud; 1030(a)(2) - Theft of Information From a Computer; 1030(a)(5)(B) - Recklessly Damaging a Computer; and Section 2 - Aiding and Abetting.

On 07/19/11, Swartz surrendered to federal authorities and was arraigned before Magistrate Judge Judith G. Dein.

Case continued in Boston.

**DETAILS OF INVESTIGATION:**

Reference is made to all previous reports in this case, the most recent of which is the Report of Continuing Investigation written by SA (b)(6),(b)(7)(C) on 06/29/11.

**JUDICIAL ACTION:**

On 07/14/11, Swartz was indicted in U.S. District Court for the District of Massachusetts for violations of Title 18 United States Code, Sections 1343 - Wire Fraud; 1030(a)(4) - Computer Fraud; 1030(a)(2) - Theft of Information From a Computer; 1030(a)(5)(B) - Recklessly Damaging a Computer; and 2 - Aiding and Abetting.

On 07/19/11, Swartz surrendered to federal authorities and was arraigned before Magistrate Judge Judith G. Dein. Swartz was released on \$100,00.00 bond.

**SUSPECTS / DEFENDANTS:**

**SWARTZ, Aaron - DEFENDANT - ARRESTED (FEDERAL)**

1599: Yes

1599A: No

**(b)(6),(b)(7)(C)** - SUBJECT

1599: Yes

1599A: No

**(b)(6),(b)(7)(C)** SUBJECT

1599: Yes

1599A: No

**EXAMS CONDUCTED:**

**ECSAP:** 05/20/11

**Poly:** N/A

**PSD:** N/A

**DATABASE SEARCHES CONDUCTED:**

**MCI / CI:** 01/07/11

**NCIC/NLETS:** 01/07/11

**CCS/CPT:** 01/07/11

**LOCAL LE:** 01/07/11

**EVIDENCE / CONTRABAND / PERSONAL PROPERTY:**

All evidence remains secured in the Boston Field Office Evidence vault as previously reported.

**DISPOSITION:**

Case continued pending further investigation and judicial action.

**USSS / BOSTON**

**(b)(6),(b)(7)(C)** RICCIARDI

ORIGINAL

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

From: BOS  
Sent: Tuesday, November 29, 2011 3:49 PM  
To: CID  
Cc: ISD; BOS  
Subject: 775.510 Aaron Swartz J-102-775-60071-S (Continued)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE  
TO: CRIMINAL INVESTIGATIVE DIVISION  
INFO: INVESTIGATIVE SUPPORT DIVISION  
SUBJECT: REPORT OF CONTINUING INVESTIGATION  
FILE: J-102-775-60071-S  
X-REF: N/A  
SEIZURE#: N/A

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)  
DATE CASE OPENED: 01/07/11  
PREVIOUS REPORT: 08/01/11 - NOTIFICATION OF FEDERAL ARREST  
REPORTING PERIOD: 08/02/11 - 11/29/11  
STATUS: CONTINUED

SYNOPSIS:

In addition to the federal charges pending in this case, Aaron Swartz was also indicted in Suffolk County, MA Superior Court for state charges to include breaking and entering in the daytime with intent to commit a felony, larceny over \$250 and unauthorized access to a computer network.

Case continued in Boston.

DETAILS OF INVESTIGATION:

Reference is made to all previous reports in this case, the most recent of which is the Report of Continuing Investigation written by SA (b)(6),(b)(7)(C) dated 08/01/11.

On 11/21/11, Aaron Swartz, along with attorneys Martin Weinberg and (b)(6),(b)(7)(C) came to the Boston Field Office to review evidence in this case as part of the discovery process. After the review, items approved for release by AUSA Stephen Heymann were turned over to attorney Weinberg.

On 11/23/11, SA (b)(6),(b)(7)(C) turned over the Apple iMac model A1311 with serial number WB025AXGDA7 that was seized from Harvard University pursuant to a federal search warrant on 02/11/11 to (b)(6),(b)(7)(C) of the Harvard University Police Department.

JUDICIAL ACTION:

On 11/17/11, Aaron Swartz was indicted in Suffolk Superior Court for two counts of breaking and entering in the daytime with intent to commit a felony, larceny over \$250, and three counts of unauthorized access to a computer network.

On 11/25/11, Assistant District Attorney **(b)(6),(b)(7)(C)** for the Middlesex District Attorney's Office emailed SA **(b)(6),(b)(7)(C)** to inform him that he expected Swartz to be arraigned on 11/30/11.

**SUSPECTS / DEFENDANTS:**

**SWARTZ, Aaron - DEFENDANT - ARRESTED (FEDERAL)**

1599: Yes  
1599A: Yes  
PHOTO: Yes  
PRINTS: Yes

**(b)(6),(b)(7)(C)** - SUBJECT

1599: Yes  
1599A: No

**(b)(6),(b)(7)(C)** - SUBJECT

1599: Yes  
1599A: No

**EXAMS CONDUCTED:**

ECSAP: 05/20/11  
Polygraph: N/A  
PSD: N/A

**DATABASE SEARCHES CONDUCTED:**

NCI / CI: 01/07/11  
NCIC/MLSTS: 01/07/11  
CCS/CFT: 01/07/11  
LOCAL LE: 01/07/11

**EVIDENCE / CONTRABAND / PERSONAL PROPERTY:**

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 31  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA **(b)(6),(b)(7)(C)**  
**DESCRIPTION OF ITEMS:** Scientific Atlantic Modem SN# SM1565968  
Apple Multi Adapter SN# 6F9395M72U6  
Apple Multi Adapter SN# 6F7281NNU49  
Black Notebook Journal  
**SEIZED / OBTAINED FROM:** Aaron Swartz  
**LOCATION:** Boston Field Office Evidence Vault  
**DISPOSITION:** Item 1 and 4 returned to Swartz's attorney, Martin Weinberg, on 11/21/11.

**EVIDENCE SSF 1544 S/N:** 102 2011 CE 32  
**DATE OF INVENTORY:** 02/11/11  
**INVENTORY MADE BY:** SA **(b)(6),(b)(7)(C)**  
**DESCRIPTION OF ITEMS:** Harvard University Warning Statement  
Warning Statement Addressed to Aaron Swartz  
Master's Thesis M-876 Lind  
Western Digital Mail-in Rebate Form

**SEIZED / OBTAINED FROM:** Aaron Swartz  
**LOCATION:** Boston Field Office Evidence Vault

**DISPOSITION:**

Items 1 - 5 returned to Swartz's attorney, Martin Weinberg, on 11/21/11.

**EVIDENCE SSF 1544 S/N:**

102 2011 CE 33

**DATE OF INVENTORY:**

02/11/11

**INVENTORY MADE BY:**

SA (b)(6)/(b)

**DESCRIPTION OF ITEMS:**

Wireless-G 2.4 GHz Broadband Router Linksys  
MacBook Mac OSX Install Disc one and two  
MacBook User Guide in Gray Cardboard case  
Apple Care Service Letter Dispatch R&275408  
Genius Bar Work Confirmation

**SEIZED / OBTAINED FROM:**

Aaron Swartz

**LOCATION:**

Boston Field Office Evidence Vault

**DISPOSITION:**

Item 1 returned to Swartz's attorney, Martin Weinberg, on 11/21/11.



EVIDENCE SSF 1544 S/N: 102 2011 CE 35  
 DATE OF INVENTORY: 02/11/11  
 INVENTORY MADE BY: SA (b)(6), (b)(7)(C)  
 DESCRIPTION OF ITEMS: Metallic Blue iPod  
 White iPod with carrying case  
 White iPod with serial number SA633065UX8A  
 White iTalk  
 Black 16GB Thumb-drive  
 SEIZED / OBTAINED FROM: Aaron Swartz  
 LOCATION: Boston Field Office Evidence Vault  
 DISPOSITION: Items 1 - 5 returned to Swartz's attorney, Martin Weinberg, on 11/21/11.

EVIDENCE SSF 1544 S/N: 102 2011 CE 36  
 DATE OF INVENTORY: 02/11/11  
 INVENTORY MADE BY: SA (b)(6), (b)(7)(C)  
 DESCRIPTION OF ITEMS: Fifty-four miscellaneous compact discs  
 Two hard drive enclosures  
 T-Mobile Sidekick  
 Sony Micro Vault  
 SEIZED / OBTAINED FROM: Aaron Swartz  
 LOCATION: Boston Field Office Evidence Vault  
 DISPOSITION: 39 CDs returned to Swartz's attorney, Martin Weinberg, on 11/21/11.

EVIDENCE SSF 1544 S/N: 102 2011 CE 37  
 DATE OF INVENTORY: 02/11/11  
 INVENTORY MADE BY: SA (b)(6), (b)(7)(C)  
 DESCRIPTION OF ITEMS: DVD-R with handwritten label  
 Pocket notebook  
 Pure Drive Quick start guide  
 Disk utility internal hard drive upgrade kit  
 Seagate Barracuda Hard Drive Installation Guide  
 SEIZED / OBTAINED FROM: Aaron Swartz  
 LOCATION: Boston Field Office Evidence Vault  
 DISPOSITION: Items 3 - 5 returned to Swartz's attorney, Martin Weinberg, on 11/21/11.

EVIDENCE SSF 1544 S/N: 102 2011 CE 38  
 DATE OF INVENTORY: 02/11/11  
 INVENTORY MADE BY: SA (b)(6), (b)(7)(C)  
 DESCRIPTION OF ITEMS: Apple iMac Model A1311 serial number WB025AXGD87  
 Western Digital Hard Drive SN WMANN1006724  
 SEIZED / OBTAINED FROM: Aaron Swartz  
 LOCATION: Boston Field Office Evidence Vault  
 DISPOSITION: Item 1 turned over to Harvard Univ. Prof. (b)(6), (b)(6), (b)(7)(C) on 11/23/11.

EVIDENCE SSF 1544 S/N: 102 2011 CE 81  
 DATE OF INVENTORY: 02/25/11  
 INVENTORY MADE BY: SA (b)(6), (b)(7)(C)  
 DESCRIPTION OF ITEMS: 16 CD contained in a mailing envelope  
 SEIZED / OBTAINED FROM: Aaron Swartz  
 LOCATION: Martin Weinberg P.C.  
 DISPOSITION: Returned to Swartz's attorney, Martin Weinberg, on 11/21/11.

**DISPOSITION:**

Case continued pending further investigation and judicial action.

USSS/BOSTON

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

/ RICCIARDI

ORIGINAL

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

From: BOS  
Sent: Monday, February 27, 2012 6:01 PM  
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 FILE: 102-775-60071-S  
TO: CRIMINAL INVESTIGATIVE DIVISION X-REF: N/A  
INFO: INVESTIGATIVE SUPPORT DIVISION SEIZURE#: N/A  
SUBJECT: REPORT OF CONTINUING INVESTIGATION

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)  
DATE CASE OPENED: 01/07/11  
PREVIOUS REPORT: 11/29/11 - Report of Continuing Investigation  
REPORTING PERIOD: 11/30/11 - 02/27/11  
STATUS: CONTINUED

SYNOPSIS:

Swartz was arraigned in the Middlesex County, Massachusetts Superior Court on two counts of breaking and entering in the daytime; one count of larceny for more than \$250.00; and three counts of unauthorized access to a computer.

Case continued in Boston.

DETAILS OF INVESTIGATION:

Reference is made to all previous reports in this case, the most recent of which is the Report of Continuing Investigation written by SA (b)(6),(b)(7)(C) on 11/29/11.

On 12/20/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) Cambridge PD, and Detective (b)(6),(b)(7)(C) Boston PD (both of the New England Electronic Crimes Task Force - NEECTF) delivered a hard drive containing discovery information prepared by (b)(6),(b)(7)(C) of CERT to 20 Park Plaza in Boston, Massachusetts. The drive was signed for by (b)(6),(b)(7)(C) of Martin Weinberg P.C. The signed receipt by (b)(6),(b)(7)(C) will remain a permanent part of this case file.

On 01/31/12 (b)(6),(b)(7)(C) a courier for Martin Weinberg, signed for a Toshiba Portable Hard Drive containing discovery information also prepared by (b)(6),(b)(7)(C) at the Boston Field Office.

JUDICIAL ACTION:

On 11/30/11, Swartz was arraigned in Middlesex County, Massachusetts Superior Court on two counts of breaking and entering daytime, one count of larceny for more than \$250.00, and three counts of unauthorized access to a computer.

**SUSPECTS / DEFENDANTS:**

**AARON H SWARTZ - DEFENDANT**

1599:	Yes
1599A:	Yes

**EXAMS CONDUCTED:**

**ECSAP:** 05/20/11

**Poly:** N/A

**FSD:** N/A

**DATABASE SEARCHES CONDUCTED:**

**MCI / CI:** 01/07/11

**NCIC/NLETS:** 01/07/11

**CCB/CFT:** 01/07/11

**LOCAL LE:** 01/07/11

Results of database searches have been reported under "Details of Investigation".

**EVIDENCE / CONTRABAND / PERSONAL PROPERTY:**

All evidence remains in the Boston Field Office Evidence Vault.

**DISPOSITION:**

Case continued pending further investigation and judicial action.

**USSS/BOSTON**

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

**RICCIARDI**

ORIGINAL

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

From: BOS  
Sent: Tuesday, May 29, 2012 2:11 PM  
To: CID  
Cc: BOS; ISD  
Subject: CT 775.510 Aaron Swartz (J-102-775-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE FILE: J-102-775-60071-S  
TO: CRIMINAL INVESTIGATIVE DIVISION X-REF: N/A  
INFO: INVESTIGATIVE SUPPORT DIVISION SEIZURE#: N/A  
SUBJECT: REPORT OF JUDICIAL ACTION

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)  
DATE CASE OPENED: 01/07/11  
PREVIOUS REPORT: 02/27/12 - Report of Continuing Investigation  
REPORTING PERIOD: 02/28/12 - 05/29/12  
STATUS: CONTINUED

SYNOPSIS:

Judicial action continues in the case of the United States versus Aaron Swartz and the case of the Commonwealth of Massachusetts versus Aaron Swartz.

Case continued in Boston.

DETAILS OF INVESTIGATION:

Reference is made to all previous reports in this case, the most recent of which is the Report of Continuing Investigation written by SA (b)(6),(b)(7)(C) on 02/27/12.

Reference is made to the telephone conference between Assistant U.S. Attorney Stephen Heymann, SA (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) Cambridge Police Department on 05/15/12.

Reference is made to the email from Assistant District Attorney (b)(6),(b)(7)(C) to SA (b)(6),(b)(7)(C) on 05/23/12.

JUDICIAL ACTION:

On 05/15/12, AUSA Heymann, Detective (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) conducted a telephone conference call to discuss the progress of the case against Swartz. AUSA Heymann informed SA (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) that the case was progressing and he expected judicial action at some time in the future.

SUSPECTS / DEFENDANTS:

**AARON H SWARTZ - DEFENDANT**

1599: Yes  
1599A: Yes

**XAMS CONDUCTED:**

**ECSAP: 05/20/11**

**Poly: N/A**

**FSD: N/A**

**DATABASE SEARCHES CONDUCTED:**

NCI / CI: 01/07/11  
NCIC/MLTS: 01/07/11  
CCS/CFT: 01/07/11  
LOCAL LE: 01/07/11

Results of database searches have been reported under "Details of Investigation."

**EVIDENCE / CONTRABAND / PERSONAL PROPERTY:**

All remaining evidence is in the Boston Field Office Evidence Vault.

**DISPOSITION:**

Case continued pending further investigation and judicial action.

**USSS/BOSTON**

**(b)(6),(b)(7)(C) / RICCIARDI**

On 09/18/12, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) AUSA Stephen Heymann and AUSA (b)(6),(b)(7)(C) interviewed the following Massachusetts Institute of Technology employees in furtherance of trial preparation: (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C) at 77 Massachusetts Avenue, Cambridge, Massachusetts.

**JUDICIAL ACTION:**

On 09/12/12, a superseding indictment was rendered in the United States District Court, District of Massachusetts, charging Aaron Swartz with violations of 18 U.S.C 1343 wire fraud; 18 U.S.C 1030 computer fraud, unlawfully obtaining information from a protected computer and recklessly damaging a protected computer; and 18 U.S.C 2 aiding and abetting.

**SUSPECTS / DEFENDANTS:**

AARON H SWARTZ - DEFENDANT

1599: Yes  
1599A: Yes

**XAMS CONDUCTED:**

ECSAP: 05/20/11

Poly: N/A

FSD: N/A

**DATABASE SEARCHES CONDUCTED:**

NCI / CI: 01/07/11  
NCIC/MLETS: 01/07/11  
CCS/CFT: 01/07/11  
LOCAL LE: 01/07/11

**EVIDENCE / CONTRABAND / PERSONAL PROPERTY:**

All remaining evidence is in the Boston Field Office Evidence Vault.

**DISPOSITION:**

Case continued pending further investigation and judicial action.

USSS/BOSTON

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



**(CD)**

ORIGINAL

BOS  
Thursday, January 17, 2013 8:59 AM  
CID  
ISD; BOS  
CT 775.510 Aaron Swartz (J-102-775-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT  
BOSTON FIELD OFFICE

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

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

SUBJECT: REPORT OF JUDICIAL ACTION

**ACTUAL LOSS: TBD**

POTENTIAL LOSS: \$2,000,000.00

POTENTIAL 1

CASE TITLE:  
CASE TYPE:  
SECONDARY TYPES:  
CONTROLLING OFFICE:  
REPORT MADE BY:  
DATE CASE OPENED:  
PREVIOUS REPORT:  
REPORTING PERIOD:  
STATUS:

AARON SWARTZ  
775.510  
848.191, 848.304, 848.930  
BOSTON FIELD OFFICE  
SA [REDACTED] (b)(6), (b)(7)(C)  
01/07/11  
09/21/12 -  
09/22/12 - 1/17/13  
CONTINUED

SYNOPSIS

**SYNOPSIS:**

On 1/11/13, Aaron Swartz was found dead in his apartment in Brooklyn, NY as a result of an apparent suicide.

A suppression hearing in this had been scheduled for 4/01/13, in U.S. District Court.

A suppression hearing in this had been scheduled for 1/25/13, with a trial date of 4/01/13, in U.S. District Court for the District of Massachusetts.

Case continued.

DETAILS OF THE

**DETAILS OF INVESTIGATION:**

Reference is made to all previous reports in this case, the most recent of which is the Report Judicial Action written by SA [redacted] on 09/21/12.

On 1/12/13, several open internet sources were searched.  
Swartz. Detective (b)(8), (b)(7)(C)  
York City PD (b)(6), (b)(7)(C)

On 1/12/13, several open internet sources were reporting the death of Aaron Swartz. Detective [REDACTED] Cambridge, MA PD, contacted Detective [REDACTED] New York City PD (NYPD) - Precinct 71 to confirm Swartz' death. Detective [REDACTED] stated that at 19:35 hours on 1/11/13, it was reported to NYPD that Aaron Swartz had committed suicide. Detective [REDACTED] further stated he responded to [REDACTED] and confirmed that Aaron Swartz was found dead of an apparent accident. The reporting party was Swartz. [REDACTED]

(C) [REDACTED] (b)(6), (b)(7)(C)

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

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

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

**JUDICIAL ACTION:**

A suppression hearing had been scheduled for 1/25/13 in U.S. District Court for the District of Massachusetts with a trial date of 4/01/13.

**SUSPECTS / DEFENDANTS:**

AARON H SWARTZ - DEFENDANT (FEDERAL)  
1599: Yes (Entered 1/19/2011)  
1599A: Yes (Entered 11/29/2011)

**EXAMS CONDUCTED:**

ECSAP: 05/20/11  
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 remains in the Boston Field Office Evidence Vault as previously reported.

**DISPOSITION:**

Case continued pending disposition of evidence.

USSS / BOSTON

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

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

(CID)

ORIGINAL

From:  
Sent:  
To:  
Cc:  
Subject:

BOS  
Tuesday, June 25, 2013 3:09 PM  
CID  
BOS; ISD  
775.510 Aaron Swartz (J-102-813-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

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

FILE: J-102-813-60071-S  
X-REF: N/A  
SEIZURE NO: N/A

SUBJECT: REPORT OF CONTINUING INVESTIGATION

CASE TITLE:  
CASE TYPE:

SECONDARY CASE TYPE:  
CONTROLLING OFFICE:  
REPORT MADE BY:  
DATE CASE OPENED:  
PREVIOUS REPORT:  
REPORTING PERIOD:  
STATUS:

AARON SWARTZ  
775.510 - NETWORK INTRUSION OR COMPUTER HACK/  
UNIVERSITIES  
848.191; 848.304; 848.930  
BOSTON FIELD OFFICE (617-565-5640)  
SA (b)(6),(b)(7)(C)  
01/07/11  
REPORT OF JUDICIAL ACTION, DATED 01/17/13  
01/18/13 - 06/25/13  
CONTINUED

SYNOPSIS:

On 03/18/13, Assistant United States Attorney (AUSA) Stephen Heymann instructed this agent to return most of the property seized from Aaron Swartz to his family's attorney, (b)(6),(b)(7)(C). The property was returned as directed.  
Case continued pending disposition of remaining evidence.

DETAILS OF INVESTIGATION:

Reference is made to all previous reports in this case, the last a Report of Judicial Action written by SA (b)(6),(b)(7)(C) dated 01/17/13.  
There are no details of investigation to report during this reporting period.

JUDICIAL ACTION:

On 03/18/13, AUSA Stephen Heymann contacted this agent and authorized the return of all of Aaron Swartz's property that was being held in this case except for his laptop.  
Continuing on 03/18/13, (b)(6),(b)(7)(C) legal assistant to Attorney (b)(6),(b)(7)(C) picked up all remaining evidence except for Swartz's laptop. A receipt of returned property was signed and will remain a part of this case file.

**SUSPECTS/DEFENDANTS:**

AARON H SWARTZ - DEFENDANT - (FEDERAL) - DECEASED  
SSF 1599: YES (Entered 01/19/11)  
SSF 1599A: YES (Entered 11/29/11)

**EXAMS CONDUCTED:**

ECSAP: 05/20/11  
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:**

EVIDENCE SSF 1544 S/N: 102 2011 CE 000031  
DATE OF INVENTORY: 02/11/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)  
DESCRIPTION OF ITEMS: 2 Apple Multi-Adapters  
SEIZED / OBTAINED FROM: 950 Massachusetts Ave # 320 Boston  
DISPOSITION: Returned to Atty. (b)(6),(b)(7)(C)

EVIDENCE SSF 1544 S/N: 102 2011 CE 000033  
DATE OF INVENTORY: 02/11/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)  
DESCRIPTION OF ITEMS: MacBook Install Disks, User Guide,  
Service Letters, Flashcard  
SEIZED / OBTAINED FROM: 950 Massachusetts Ave # 320 Boston  
DISPOSITION: Returned to Atty. (b)(6),(b)(7)(C)

EVIDENCE SSF 1544 S/N: 102 2011 CE 000034  
DATE OF INVENTORY: 02/11/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)  
DESCRIPTION OF ITEMS: Nokia Cell Phone, HTC G2, 12 Media  
Tapes  
SEIZED / OBTAINED FROM: 950 Massachusetts Ave # 320 Boston  
DISPOSITION: Returned to Atty. (b)(6),(b)(7)(C)

EVIDENCE SSF 1544 S/N: 102 2011 CE 000036  
DATE OF INVENTORY: 02/11/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)  
DESCRIPTION OF ITEMS: Sideskick, Sony Microvault  
SEIZED / OBTAINED FROM: 950 Massachusetts Ave # 320 Boston  
DISPOSITION: Returned to Atty. (b)(6),(b)(7)(C)

EVIDENCE SSF 1544 S/N: 102 2011 CE 000037  
DATE OF INVENTORY: 02/11/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)  
DESCRIPTION OF ITEMS: DVD, Pocket Notebook  
SEIZED / OBTAINED FROM: 950 Massachusetts Ave # 320 Boston

**DISPOSITION:**

Returned to Atty. (b)(6),(b)(7)(C)

EVIDENCE SSF 1544 S/N: 102 2011 CE 000038  
DATE OF INVENTORY: 02/11/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)  
DESCRIPTION OF ITEMS: Western Digital HDD  
SEIZED / OBTAINED FROM: 950 Massachusetts Ave # 320 Boston  
DISPOSITION: Returned to Atty. (b)(6),(b)(7)(C)

EVIDENCE SSF 1544 S/N: 102 2011 CE 000062  
DATE OF INVENTORY: 02/11/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)  
DESCRIPTION OF ITEMS: Galaxy External HDD  
SEIZED / OBTAINED FROM: 950 Massachusetts Ave # 320 Boston  
DISPOSITION: Returned to Atty. (b)(6),(b)(7)(C)

EVIDENCE SSF 1544 S/N: 102 2011 CE 000038  
DATE OF INVENTORY: 02/11/11  
INVENTORY MADE BY: SA (b)(6),(b)(7)(C)  
DESCRIPTION OF ITEMS: Apple iMac WB025AXGD87  
SEIZED / OBTAINED FROM: 950 Massachusetts Ave # 320 Boston  
LOCATION: Boston Evidence Vault  
DISPOSITION: Held pending instruction from USAO

**DISPOSITION:**

Case continued pending disposition of remaining evidence.

USSS/BOSTON

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

/RICCIARDI

## INVESTIGATIVE TRAVEL WORKSHEET

Name of Traveler: Det (b)(6),(b)(7)(C) Cambridge, MA PD (Task Force Officer)  
Traveling From: Boston, MA  
Traveling To: New York, NY  
Method of Travel: Train  
Dates of Travel: 01/13/12 - 01/15/12  
Case Number: J-102-775-60071-S  
Case Title: Aaron Swartz  
AUSA / District Attorney: AUSA Stephen Heymann  
Court District: District of Massachusetts

### REFERENCED CONVERSATIONS

*Foreign Travel Requires GS-15 Approval*

Reference the telephone conversation between ATSAIC (b)(6),(b)(7)(C) (BOS) and ATSAIC (b)(6),(b)(7)(C) (NYC) on 01/04/12 regarding this travel.

Supervisor / Office of Traveler: ATSAIC (b)(6),(b)(7)(C) (BOS)

Supervisor / Office of Destination: ATSAIC (b)(6),(b)(7)(C) (NYC)

Purpose of Travel: Cambridge, MA Det (b)(6),(b)(7)(C) a member of the New England Electronic Crimes Task Force (NEECTF) is being requested to travel to New York along with (2) AUSA's from the District of Massachusetts (AUSA Stephen Heymann and AUSA Scott Garland) from 1/13/13 - 1/15/13 to interview witnesses in preparation for a trial in case #J-102-775-60071-S. See attached SSF 4000, Invitational Travel Request/Authorization for Non-Employees

# INVITATIONAL TRAVEL REQUEST/AUTHORIZATION FOR NON-EMPLOYEES

(If additional space is needed use back of this form)

INSTRUCTIONS: All invitational travel requests must be approved by the originating office's Assistant Director or Chief Counsel; forwarded to the Assistant Director of Administration through the SAIC, LRC; and include the name(s) and title(s) of the traveler(s), organization(s) of the traveler(s), dates of travel, purpose of travel, and type of travel and/or per diem required, to include origin and destination of travel. All elements of the approval process should be accomplished prior to the onset of travel.

Authority for invitational travel is authorized in accordance with 5 U.S.C. 5731(a), 5703 and 5704, and the Federal Travel Regulations as implemented by the U.S. Secret Service.

1) REQUESTED BY (Name/Division/Office):

ATSAIC (b)(6), (b)(7)(C) BOS

2) NAME, TITLE, AND ORGANIZATION OF TRAVELER(S):

Task Force Officer (TFO) (b)(6), (b)(7)(C) (DOB: (b)(6), (b)(7)(C) Cambridge, MA Police Department

2a) IS THE TRAVELER(S) A CONTRACTOR? ☐ YES ☒ NO

3) PURPOSE OF TRAVEL AND EXPLANATION OF THE BENEFIT TO THE SERVICE:

Cambridge, MA De (b)(6), (b)(7)(C) a member of the New England Electronic Crimes Task Force (NEECTF), is being requested to travel to New York along with (2) AUSA's from the District of Massachusetts (AUSA Stephen Heymann and AUSA Scott Garland) from 1/13/13 - 1/15/13 to interview witnesses in preparation for a trial in case #J-102-775-40071-8. A federal trial is scheduled for February 2013 for main suspect Aaron Swartz who was indicted in the spring of 2012.

4) EXPENSES TO BE AUTHORIZED (Mark "X" in appropriate box(es)):

☒ TRAVEL ☒ LODGING ☒ PER DIEM ☐ OTHER (Explain) \_\_\_\_\_

NOTE: The Logistics Resource Center (LRC) will fill in authorized rates.

5) ITINERARY (include origin and destination of travel):

1/13/13 - Depart Boston, MA via Amtrak train / Arrive New York, NY (RON)  
1/14/13 - Conduct interviews in New York, NY (RON)  
1/15/13 - Conduct interviews in New York, NY / Depart New York, NY via Amtrak train / Arrive Boston, MA

6) PROJECT CODE TO BE CHARGED:

7) AD'S SIGNATURE OR CHIEF COUNSEL (Originating Office):

(Print name)

(Signature)

(Date)

## LRC USE ONLY

AUTHORIZATION NUMBER:

EFFECTIVE DATES OF TRAVEL:

## APPROVALS (Logistics Resource Center and AD-Administration)

SIGNATURE OF SAIC-LRC:

DATE:

SIGNATURE OF AD-ADMINISTRATION:

DATE:

NOTE: THE LOGISTICS RESOURCE CENTER STAFF WILL COMPLETE THE AUTHORIZATION CITING THE AUTHORIZATION NUMBER, PER DIEM, LODGING RATES, AND OTHER PERTINENT INFORMATION NEEDED FOR THE TRAVELER TO VOUCHER HIS/HER EXPENSES TO THE SECRET SERVICE. AUTHORIZATION WILL THEN BE SENT TO THE AD-ADMINISTRATION FOR SIGNATURE AND FINAL APPROVAL. EXPENSES SHOULD BE VOUCHERED DIRECTLY TO THE U.S. SECRET SERVICE BY THE TRAVELER AS SOON AS THE TRAVEL IS COMPLETE. THIS COMPLETED AUTHORIZATION WILL BE ATTACHED TO THE TRAVEL VOUCHER.

(CONTINUATION PAGE FOR INVITATIONAL TRAVEL REQUEST/AUTHORIZATION FOR NON-EMPLOYEES)

UNITED STATES SECRET SERVICE

SSF 4006 (Rev 05/2006)

**RIF**

407



//ROUTINE//

FROM: SAIC - Criminal Investigative Division

File: 400.090

TO: SAIC - New York Field Office  
SAIC - Boston Field Office

INFO: AD - Office of Investigations  
Chief - Financial Management Division

SUBJECT: Invitational Travel of TFO (b)(6),(b)(7)(C) New England  
Electronic Crimes Task Force, to New York City, NY from 01/13/13 -  
01/15/13

Reference is made to the 01/08/13 communications between ATSAIC (b)(6),(b)(7)(C) (BOS), ATSAIC (b)(6),(b)(7)(C) (NYC), ATSAIC (b)(6),(b)(7)(C) (CID), and SA (b)(6),(b)(7)(C) (CID) regarding this travel.

Final reference is made to the SSF 4000, Invitational Travel Request/Authorization for Non-Employees, approved by DAD Hugh Dunleavy (INV) and SAIC Carrie Hunnicutt (ADM) authorizing this travel.

TFO (b)(6),(b)(7)(C) is authorized to travel via Amtrak from Boston, MA to New York City, NY. TFO (b)(6),(b)(7)(C) at the request of Assistant United States Attorney (AUSA) Stephen Heymann, District of Massachusetts, will interview witnesses in preparation for trial in case #J-102-775-60071-S (Aaron Swartz).

Schedule for TFO (b)(6),(b)(7)(C) is as follows:

01/13/13 - Travel to New York City  
01/14/13 - Conduct Interviews  
01/15/13 - Conduct Interviews / Return travel to POD

Appropriate liaison has been established with the New York Field Office. ATSAIC (b)(6),(b)(7)(C) (BOS) will make all appropriate travel and lodging arrangements.

Invitational travel number, 13-26, should be used for all travel related travel documentation.

All personnel are reminded of the Director's recommendations regarding better business practices in utilizing Secret Service funds to include travel for protective missions, investigations and training. When traveling to or from cities with multiple airports, SATO will provide a cost comparison. All personnel are expected to use the most cost effective airport while considering taxi rates to your destination.

Questions regarding this travel should be directed to ATSAIC (b)(6),(b)(7)(C) (CID) at (b)(6),(b)(7)(C)

Headquarters (CID) (b)(6),(b)(7)(C)

MCI(070) SUBJECT DESCRIPTION  
SUBJ D CASE NR 102-775-0060071-S SUBJ NR 1 CFO 102 CASE TYPE 775510

CRHIS EVID ADDNO EMPY FAMLY SSUM CSUM  
NAME(L,F,M) SWARTZ AARON AFFIX A/D J CASE  
SEX RACE HGT WGT EYES HAIR DOB POB:CITY ST CTRY CITIZENSHIP  
M W 506 120 BRO BRO 11081986 CHICAGO IL US  
INTEREST CODES 38 13 OCCUPATION CODES  
DECEASED DEFENDANT

DO NOT SEND TO TEGS: KNOWN TO SA: (b)(6),(b)(7)(C)  
SSN (b)(6),(b)(7)(C) 493 FBI NO 675304KDO  
MIL.SR-BRCH PASS.CTRY US NO (b)(6),(b)(7)(C)  
ID NO/ST PD MA 10556559 D/L ST NO  
SCARS/MARKS INS ALIEN NO  
SPEECH DEFECT TATTOOS  
MISSING LIMB ACCENT  
NATIONALITY PHY DEFORMITY  
AFIS NO ADDICT  
HAND/W MMDDYY PHOTO 010411 FINGER/P 010411 PALM/P MMDDYY  
REMARKS DATE EST 011911 DATE UPD 011813

MCI(311NEW) FINANCIAL CRIMES INVESTIGATION  
CCTRL D CASE NUMBER: 102-775-0060071-S CC NR: 2 CASE TYPE: 775.510  
SARS CASE(Y/N):

CCTRL HAS NO ADDITIONAL SECONDARY  
OFF: 178 CASE TITLE: AARON SWARTZ

CPG TYPE:

PRIMARY	LOCATION-----	FIELD	CID REGION ONE			AGENT	AGENT	AGENT	DATE
UNITS	ST CITY	ORIG	100	ZONE	7D NR	OFF	OFF	ASSIGNED	
1	DC CID		X		000001	178	178	013111	

DEVICES PRIOR TO 12/01/12- CURRENT POTENTIAL DOLLAR LOSS:  
CURRENT ACTUAL DOLLAR LOSS:  
QUANTITIES BY TYPE----- TOTAL QUANTITY BY TYPE-  
CRED CARD DEBIT CARD PREPAID CARD COMM CARD BANK ACCT BROKE ACCT COMMR ACCT

WIRE TRAN TRAVL CHK BROKE CHCK COMM CHK PERS CHK E-MONEY OTHER

----- CLOSING AND JUDICIAL ACTION -----  
DATE CLOSED OFFENDER ID ACCEPT BLANKET DECLINE SPECIFIC DECLINE  
MMDDYY Y/N: FEDRL: FEDRL: FEDRL:  
STATE: STATE: STATE:

REMARKS:

F3	F4	F5	F6	F9	F10	DATE EST 013111
CASE	TICK	SECD	JUST	MENU	EXIT	DATE UPD 013111

MCI(070) SUBJECT DESCRIPTION  
SUBJ D CASE NR 102-775-0060071-S SUBJ NR 1 CFO 102 CASE TYPE 775510

CRNIS EVID ADDNO EMPLOY FAMILY SSUM CSUM  
NAME(L,F,M) SWARTZ AARON AFFIX A/D J CASE  
SEX RACE HGT WGT EYES HAIR DOB POB:CITY ST CTRY CITIZENSHIP  
M W 506 120 BRO BRO 11081986 CHICAGO IL US  
INTEREST CODES 38 13 OCCUPATION CODES  
DECEASED DEFENDANT

DO NOT SEND TO TECS: KNOWN TO SA: (b)(6),(b)(7)(C)  
SSN (b)(6) 0493 FBI NO 675304KDO  
MIL.SR-BRCH ID NO/ST PD MA 10556559 PASS.CTRY US NO (b)(6),(b)(7)(C)  
SCARS/MARKS D/L ST NO  
SPEECH DEFECT INS ALIEN NO  
MISSING LIMB TATTOOS  
NATIONALITY ACCENT  
AFIS NO PHY DEFORMITY  
HAND/W MMDDYY PHOTO 010411 FINGER/P 010411 PALM/P MMDDYY  
REMARKS ADDICT  
DATE EST 011911 DATE UPD 011813

COMMON INDEX (CI)  
NAME: SWARTZ, AARON

NAME SEARCH RESPONSE

LAST

SEX: RACE: DOB: MMDDYY SSN: CFO:

SYSTEM CASE NUMBER

MC 1027750060071S

NAME

SWARTZ AARON

S/D SRT DOB SSN CF

\*D MWT 110886 (b)(6), 0493 (b)

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

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

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

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

SELECT F1-HELP F2-REFRESH F3-SUBJECT F4-ADDRESS F5-PHONE F6-VEHICLE F10-CI MENU F9-OTHER

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

(CID)

**From:** Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) [redacted]@usdoj.gov]  
**Sent:** Friday, February 25, 2011 10:01 AM  
**To:** (b)(6),(b)(7)(C) (CID)  
**Subject:** Aaron Swartz Case

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

Can you please send me one paragraph describing (b)(6),(b)(7)(C) areas of expertise and who he is employed by? Like (b)(6), is he employed by CERT which then has a contract with secret Service or like you is he an agent. Also, has he previously handled grand jury material in other criminal investigations in other districts?

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

Student  
Student  
Information  
Information  
Processing  
Processing  
Board  
Board



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



