UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Criminal No. 11-10260-NMG**
	)	
AARON SWARTZ,	)	
	)	
Defendant	)	

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.[1] To pay its expenses, JSTOR normally charges subscription

[1] 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' down-loading 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[2] and allows the guest computer network service for a

[2]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.[3] 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[4] 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 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.

[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 18.55.6.21***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.[5]

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:f***c*** rather than the prior MAC address of 00:23:5a:73:5f:f***b***.

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).[6]

[6] 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[7] 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;[8]

(5) Beginning on January 4, 2011, MIT agreed to provide, and later provided, the Secret Service copies of network logs pertaining to

[7] 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.

> 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.[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.

---

[9] 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 bicycler 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.[10] 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)[11]

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

[10] 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.

[11] Swartz's numbering convention is used here for ease of reference.

law enforcement from taking natural investigative steps to find his equipment and identify him.

The motion should be denied on several independent and self-supporting grounds. Swartz lacked a reasonable expectation of privacy in MIT's business records. As a trespasser, Swartz lacked a reasonable expectation of privacy on MIT's computer network. The Wiretap Act offers no suppression remedy for electronic communications (as opposed to oral or wire communications), and the Stored Communications Act offers no suppression remedy whatsoever. Even if the Wiretap Act offered a suppression remedy for electronic communications, MIT's network routing, addressing and switching records were not electronic communications under the statute.

As a preliminary matter, Swartz's motion should be denied to the extent that he seeks to suppress any actions taken before January 4, 2011, because neither local nor federal law enforcement officers were investigating Swartz's downloading activity before January 4, 2011, when MIT first found the laptop. None of MIT's and JSTOR's private investigative steps before then can be attributed to the Government for the purpose of Fourth Amendment or statutory analysis, and the results of any private search before January 4, 2011, cannot be suppressed.

A. Routing, Addressing and Switching Information from MIT's Computer Network

1. *Swartz Lacked a Constitutionally-Protected Reasonable Expectation of Privacy in MIT's Network Records*

Nearly any attorney involved in the criminal justice system can recite by heart the "reasonable expectation of privacy" test for determining whether government activity constitutes a search cognizable by the Fourth Amendment. Under *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring), the warrant requirement is implicated only if (1) the individual exhibited an actual (subjective) expectation of privacy, and (2) society is prepared to recognize

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,[12] 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.[13] 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

---

[12] See http://en.wikipedia.org/wiki/Aaron-Swartz (last visited Oct. 23, 2012) for his background.

[13] 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[14] – to the police.

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

[14] 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.).[15] 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.

---

[15] *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.[16] *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. LaFave, 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.

---

[16] 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 LaFave, 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.[17] 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

[17] 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).[18] 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[19]

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. Illionois*, 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

---

[18] Swartz also contends that MIT's disclosure of its routing and trafficking records violated his Fourth Amendment rights, citing *Crispin v. Christian Audigler, 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.").

[19] 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).[20]

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

[20] 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.[21] 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

[21] 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.

identifiers on the laptop, hiding it with a hard drive in a wiring closet that MIT restricted from the public by lock, key and steel doors, concealing the equipment from MIT staff and employees under a cardboard box, and moving it to under a desk in an office in the student center to avoid detection, that expectation was not an objectively reasonable one that society is prepared to accept and adopt. *See Katz*, 389 U.S. at 361. Just because you can freely walk across MIT's campus and sit in its lobbies and you can freely walk into this courthouse and sit in a courtroom, it does not follow that you can enter either facility's locked basement wiring closet. And just because you can freely walk into MIT's library or the First Circuit's library here does not mean that you are free to return whenever you want after being forcibly removed for stealing.

Investigating a crime scene for ephemenal forensic evidence before it is disturbed is fundamental to conducting a criminal investigation, both to identify suspects and eliminate those who might otherwise be wrongfully accused. The recognized need for this is nowhere more clear than when what is being examined are concealed instrumentalities of an ongoing crime.

2. A Person Whose Presence Is "Wrongful" Has No Legitimate Expectation of Privacy in Things Wrongfully Stored on a Third-Party's Premises

Swartz lacked a reasonable expectation of privacy in the wiring closet and its contents and in the office in the student center and its contents. As the First Circuit has noted, "[a]t least three cases have held that a guest in a hotel or motel room loses his reasonable expectation of privacy when his rental period has elapsed. A fortiori, one who occupied the room by just inviting himself in could create for himself no reasonable expectation of privacy." *Amezquita v. Hernandez-Colon*, 518 F.2d 8, 11 (1st Cir. 1975) (citations omitted). Here, Swartz "occupied the room by just inviting himself in," and therefore "could create for himself no reasonable

expectation of privacy." *Id.*

Like a "burglar plying his trade in a summer cabin during the off season," Swartz's presence was "wrongful," and consequently any subjective expectation of privacy he may have had would not be "one that society is prepared to recognize as 'reasonable.'" *Rakas v. Illinois*, 439 U.S. 128, 143-44, n.12 (1978) (citations omitted). "[I]ndividuals who occupy a piece of property unlawfully have no claim under the Fourth Amendment." *United States v. Curlin*, 638 F.3d 562, 565 (7th Cir. 2011) (holding that evicted tenant who remained in house had no legitimate expectation of privacy in house, bedroom in house, or closet in bedroom). Because Swartz had no legitimate expectation of privacy in MIT's basement wiring closet or student center office, no Fourth Amendment search occurred in either place.[22]

In these regards, Swartz's situation is similar to that in *United States v. McCarthy*, 77 F.3d 522 (1st Cir. 1996). In *McCarthy*, the defendant left a suitcase unlocked and open in the back room of his landlord's trailer, a room to which he did not have exclusive access, and in any

[22] *See Curlin*, 638 F.3d at 565; *see also United States v. McRae*, 156 F.3d 708, 711 (6th Cir. 1998) (holding that defendant had no legitimate expectation of privacy in a vacant house in which he had been living for a week); *United States v. Sanchez*, 635 F.2d 47, 64 (2d Cir. 1980) (refusing to suppress photographs taken from secret compartments in rear wheel wells of car parked outside defendant's apartment building for a week and to which he possessed the keys, because car was registered to someone else and defendant could not demonstrate ownership or permission to possess the car) (citing *Rakas*); *Amezquita v. Hernandez-Colon*, 518 F.2d 8, 11 (1st Cir. 1975) (holding that squatters formerly evicted from public land had no expectation of privacy in homes they unlawfully constructed there); *United States v. Ruckman*, 806 F.2d 1471, 1472-74 (10th Cir. 1986) (holding that individual lacked expectation of privacy in contents of cave in which he resided as a trespasser on federal land); *United States v. Gale*, 136 F.3d 192, 195 (D.C. Cir. 1998) (holding that 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) (holding that hotel occupant who was asked to leave by police officers acting on behalf of hotel management no longer had a reasonable expectation of privacy in hotel room).

event after he had been told to leave the trailer. *Id.* at 535. Police took the suitcase and inventoried it without a warrant. *Id.* at 528. The First Circuit upheld the search, noting that the defendant "clearly had assumed the risk that [his landlord] might consent to a search of the room (and that the search would extend to any items, like the suitcase, sitting open in plain view). Moreover, [the defendant]'s legitimate expectation argument is further undercut by the fact that he left the open suitcase in [the landlord]'s trailer after [the landlord] told [the defendant] that he and [another] had to leave." *Id.* at 535 (citations omitted).

B. MIT Consented to the Searches and Had the Right to Do So

MIT consented to the search of its own closet and the closet's contents, and MIT had the right to do so. *See, e.g.*, *Schneckloth v. Bustamonte*, 412 U.S. 218, 222 (1973) ("A search conducted pursuant to a valid consent is constitutionally permissible."); *U.S. v. Matlock*, 415 U.S. 164, 172 n.7 (1974) (a person with common authority over premises or effects can consent to search). Swartz assumed the risk that MIT would consent to the search when he attached the laptop to MIT's network switch surreptitiously and left it hidden for extended periods. *Cf. McCarthy*, *supra* (upholding search of former tenant's suitcase when invited by landlord).

C. Officers Were Lawfully Inside The Wiring Closet and Student Center Office and Could Seize The Laptop and Hard Drive Without a Warrant Because They Were in Plain View

Even if Swartz had a reasonable expectation of privacy in MIT's wiring closet and its contents or the student center office and its contents, and even if MIT had not consented to the search of its closet and office, the computer and hard drive were lawfully seized, fingerprinted, and examined because they were in plain view where officers were lawfully present and the officers had probable cause to believe that they were evidence.

1. Officers Were Inside MIT's Wiring Closet Lawfully at MIT's Request

Law enforcement officers were lawfully present in MIT's wiring closet. MIT consented to, and in fact solicited, law enforcement's presence and investigation. This is uncontested.

2. MIT Lawfully Showed Officers The Computer Equipment They Had Found Under the Cardboard Box

The Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (internal quotation marks omitted). As a result, the Fourth Amendment is not violated when private party acts on its own accord, conducts a search, and shares the results with law enforcement. *See id.* Similarly, agents who learn of evidence via a private search may reenact the original private search without violating any reasonable expectation of privacy. *See id. See also United States v. Miller*, 152 F.3d 813, 815-16 (8th Cir. 1998); *United States v. Donnes*, 947 F.2d 1430, 1434 (10th Cir. 1991).

Under these principles, MIT validly showed officers the computer equipment it had found beneath the box, and the officers lawfully recreated MIT's searches.

3. Officers May Seize Items in Plain View Upon Probable Cause to Believe that the Items are Evidence of a Crime

Once officers encountered the laptop and the hard drive in plain view, they could seize the equipment lawfully without a warrant because they had probable cause to believe that it was evidence of a computer crime. *See United States v. Paneto*, 661 F.3d 709, 713 (1st Cir. 2011) ("One such exception [to the warrant requirement] is for items in plain view. A police officer, even though he does not have a search warrant, may seize an object in plain view as long as he

has lawfully reached the vantage point from which he sees the object, has probable cause to support his seizure of that object, and has a right of access to the object itself."); *id.* at 714 ("In general terms, probable cause exists when police have sufficient reason to believe that they have come across evidence of a crime."). "The seizure of property in plain view involves no invasion of privacy and is presumptively reasonable, assuming there is probable cause to associate it with criminal activity." *Payton v. New* York, 445 U.S. 573, 587 (1980). *See also Texas v. Brown*, 460 U.S. 730 (1183) (same).

Swartz claims that his equipment was not in plain view in the wiring closet because he had hidden it under a cardboard box. There was no Fourth Amendment search when MIT employees looked under the box or when they showed police the equipment they had found there. *See supra*. But even if MIT employees had not already lifted the box to expose the computer equipment, an item in an opaque container can still be in plain view. "[S]ome containers (for example a kit of burglar tools or a gun case) by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance." *Arkansas v. Sanders*, 442 U.S. 753, 765 (1979). There is no reasonable expectation of privacy in a container that discloses its contents. *United States v. Epps*, 613 F.3d 1093 (11th Cir. 2010) (no reasonable expectation of privacy in pillowcase with pink stains evidencing exploded dye pack following bank robbery). Here, the cardboard box disclosed its contents, because the officers knew that a hacker's computer had been traced to that closet and they saw a wire running from the box to the network switch. Law enforcement officers immediately concluded that a hard drive was contained in the enclosure underneath the laptop because a USB cable went from the enclosure to the laptop and the enclosure was of a type used

to enclose external hard drives. Consequently, the cardboard box and the wire disclosed the box's contents and therefore the laptop and the hard drive were in plain view.

4. Officers May Manipulate and Search Items in Plain View Upon Probable Cause to Believe that the Items are Evidence of a Crime

Because the equipment was in plain view and the officers had probable cause to believe that the equipment was evidence of a crime, the officers also could lawfully manipulate and search the equipment without a warrant by moving it around and opening it. "When an officer seeks to manipulate an object in plain sight, the relevant inquiry becomes whether the plain view doctrine would have sustained a seizure of the object itself." *Paneto*, 661 F.3d at 713-14 (upholding officer's picking up and examining $20 bill in plain view in apartment because officer had probable cause to believe that it was the $20 bill the officer had earlier given the defendant in a drug sting) (alterations and internal quotation marks omitted) (citing *Arizona v. Hicks*, 480 U.S. 321 (1987)).

Swartz counters the First Circuit's interpretation of *Arizona v. Hicks* in *Paneto* by contending that opening the laptop and attached hard drive case violated his Fourth Amendment rights. In *Hicks* a policeman was searching an apartment under exigent circumstances for a weapon. During the search, he noticed expensive stereo equipment. Suspecting (without probable cause) that the stereo equipment was stolen, he moved some of it to read and record its serial numbers. The Supreme Court held that although the officer was lawfully present in the apartment, moving the stereo equipment to identify its serial numbers was unlawful because this search was unsupported by probable cause. In other words, probable cause to look for a weapon does not necessarily give an officer probable cause to move stereo equipment without probable

cause to believe that the stereo equipment was evidence. However, while looking for a weapon, an officer *may* move stereo equipment if he has probable cause to believe that the stereo equipment is evidence. Indeed, the Court addressed this very point:

> Justice Powell's dissent reasonably asked what it is we would have had Officer Nelson do in these circumstances. *The answer depends, of course, upon whether he had probable cause to conduct a search*, a question that was not preserved in this case. *If he had, then he should have done precisely what he did* [i.e., moved the stereo equipment for further examination].

Hicks, 480 U.S. at 329 (emphasis added).

In the present case, investigators had probable cause to believe that the computer and attached laptop were instrumentalities of a crime. They further had probable cause to believe that the equipment would bear fingerprints that would be evidence of the crime. Fingerprinting the equipment was fully consistent with *Hicks*. Indeed, as is apparent from the quotation, it would have been encouraged.

5. Swartz's Cases Concerning Searching the Contents of a Computer's Files Are Inopposite

Swartz cites four cases in his brief for the proposition that "internal examination" of the laptop by the police constituted a Fourth Amendment search. *See* Def's Motion to Suppress No. 1 at 13-14. Swartz's cases are inapposite because they concern searches of computers' electronic files, not searches of a computers' exteriors and screens. The Government does not contend that a computer in plain view can necessarily have its files searched without a warrant.[23]

[23] Swartz argues that a network scan to determine which ports (network connection points) his computer had open was a search within the meaning of the Fourth Amendment. Def.'s Motion to Suppress No. 1 at 13-14. The ports used by a computer to communicate on a network are in electronic plain view, just as are the IP addresses used by the computer to

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").[24] 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.

[24] 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).[25]

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.

---

[25] 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 24th, 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).[26] The officers' subjective

[26] *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 (8th 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 (5th 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 (5th 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 (8th 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. LaFave, *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 (7th 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. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005) (citing *United States v. Feliz*, 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, F3d. 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.[27]

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

[27] 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.[28] 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 (7th 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

[28] 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 form 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.[29] Others are even less germane narcotics cases.[30] 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

[29] *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.

[30] *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 (9th 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."); *Unites 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 (11th Cir. May 11, 2010), *rehearing and rehearing en banc denied*, 408 Fed. App'x 346 (11th Cir. 2010) (table) (distinguishing *United States v. Mitchell*, 565 F.3d 1347 (11th 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 (11th 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