UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
v.	)	No. 11-10260-NMG
AARON SWARTZ	)	

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

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

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his USB drive.[1]

2. The USB drive was seized from him on January 6, 2011, during a search of his backpack incident to his arrest on state charges of breaking and entering in violation of M.G.L. c.266, §18.

3. His arrest was unlawful because not supported by probable cause to believe that he had committed the crime of breaking and entering.

3. On February 9, 2011, Secret Service S/A Michael Pickett obtained a warrant to search the USB drive; that warrant expired before it was executed, and another warrant to search the USB drive was obtained on February 24, 2011. *See* Exhibit 29. The USB drive was subsequently searched

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

pursuant to the warrant.

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

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

THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.

LOCAL RULE 7.1(A)(2) STATEMENT

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

MEMORANDUM OF LAW

I. BACKGROUND.

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

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

> in Swartz's possession at the time he was caught and arrested minutes later appeared to be the same one he had with him on each occasion he was videotaped in the wiring closet at MIT.
>
> 26. In the backpack was the USB DRIVE. From my training and experience and information provided to me by other agents, USB drives are frequently used to store software applications, data and records, including .pdf formatted records such as those that were illegally downloaded from JSTOR. They are also frequently used to transfer records and data between computers or hard drives, such as those connected in the wiring closet to MIT's network and ones available to Swartz outside.

Exhibit 30 at 7.[2]

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

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

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

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

---

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

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

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

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

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

> (1) Whoever steals, or with intent to defraud obtains by a false pretence, or whoever unlawfully, and with intent to steal or embezzle, converts, or secretes with intent to convert, the property of another as defined in this section, whether such property is or is not in his possession at the time of such conversion or secreting, shall be guilty of larceny, and shall . . . if the value of the property stolen exceeds two hundred and fifty dollars, be punished by imprisonment in the state prison for not more than five years, or by a fine of not more than twenty-five thousand dollars and imprisonment in jail for not more than two years; or, if the value of the property stolen . . . does not exceed two hundred and fifty dollars, shall be punished by imprisonment in jail for not more than one year or by a fine of not more than three hundred dollars . . . .
>
> (2) The term "property", as used in the section, shall include money, personal chattels, a bank note, bond, promissory note, bill of exchange or other bill, order or certificate, a book of accounts for or concerning money or goods due or to become due or to be delivered, a deed or writing containing a conveyance of land, any valuable contract in force, a receipt, release or defeasance, a writ, process, certificate of title or duplicate certificate issued under chapter one hundred and eighty-five, a public record, anything which is of the realty or is annexed thereto, a security deposit received pursuant to section fifteen B of chapter one hundred and eighty-six, electronically processed or stored data, either tangible or intangible, data while in transit, telecommunications services, and any domesticated animal, including dogs, or a beast or bird which is ordinarily kept in confinement.

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

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

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

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

---

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

[4] That copying of electronically-available data is not encompassed within §30(1) is underscored by the provisions of §30(4):

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

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

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

Because Swartz's arrest was unlawful, all fruits of that unlawful arrest, including, but not limited to, his USB drive, must be suppressed.

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

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

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

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

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

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

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

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

While S/A Pickett did add some experiential generalities about what USB drives can be used for, there is nothing in the affidavit which factually connects those potential uses to the circumstances of this particular case. Such generalities are entitled to little or no weight, as the affidavit did not provide a sufficient factual basis for the Magistrate Judge to make a neutral, independent determination that the generalities recited by S/A Pickett were likely to be true with respect to the particular search for which authorization was being sought. *See, e.g., Ribeiro*, 397 F.3d at 52 (generalizations alone may not be enough to satisfy the nexus element); *Zimmerman*, 277 F.3d 416, 433 n.3 (3d Cir. 20020(expert opinion "must be tailored to the specific facts of the case to have any value"); *Schultz*, 14 F.3d at 1097 (officer's training and experience "cannot substitute for the lack of evidentiary nexus"). The affidavit failed to establish probable cause for the search of the USB drive.

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

The government has the burden to demonstrate the applicability of the good faith exception, *see, e.g., United States v. Diehl*, 276 F.3d 32, 42 (1st Cir. 2002), and unless it can meet that burden, the evidence must be suppressed. It will not be able to do so in this case. "Although weakening the exclusionary rule, the [*Leon*] Court did not defenestrate it." *United States v. Ricciardelli,* 998 F.2d 8, 15 (1st Cir. 1993). "Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996), *aff'd on rehearing*, 91 F.3d 331 (1996). The determination whether the *Leon* good faith exception should be applied in a particular case requires an "inquir[y] into the 'objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization." *United States v. Diaz,* 841 F.2d 1, 5 (1st Cir. 1998), *quoting United States v. Leon*, 468 U.S. 897, 922 n.23 (19 84).

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

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

CONCLUSION

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

Respectfully submitted,
By his attorney,

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

CERTIFICATE OF SERVICE

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

/s/ Martin G. Weinberg

Martin G. Weinberg