COMMONWEALTH OF MASSACHUSETTS

MIDDLESEX, ss.

TRIAL COURT
DISTRICT COURT DEPARTMENT
NEWTON DIVISION
NO. 0912SW03

IN RE MATTER OF SEARCH WARRANT EXECUTED ON MARCH 30, 2009 AT THE RESIDENCE OF MOVANT RICCARDO CALIXTE

MEMORANDUM IN SUPPORT OF MOTION FOR EMERGENCY RELIEF TO QUASH THE WARRANT AND FOR RETURN OF PROPERTY

I. PROCEDURAL HISTORY

On March 30, 2009, Kevin M. Christopher ("Christopher"), a Detective for the Boston College Police Department, submitted a sworn application for a Search Warrant. See Exhibit A to the declaration of Attorney Adam Kessel (hereinafter "Kessel Decl."). The application was made to Catherine M. Coughlin, Assistant Clerk-Magistrate for Middlesex County. The warrant issued, authorizing the search of movant Riccardo Calixte's dormitory room at Gabelli Hall in Boston College and the seizure of all objects capable of storing digital data, records, indicia of ownership, and other items. (Kessel Decl. Ex. B.) Christopher then executed the search warrant and seized, among other things, Mr. Calixte's cell phone, his iPod, computers, disks, and a "post-it" note on which Calixte was in the process of taking notes about the officers' actions during the search. Christopher left a Property Receipt with Mr. Calixte listing items seized during the search. (Kessel Decl. Ex. C.) The seized post-it note does not appear on that receipt.

II. STATEMENT OF FACTS

Christopher filed the sole affidavit in support of the application for the search warrant. In summary, his affidavit reported that on January 27, 2009, a Boston College police officer filed a report regarding two students who were having "domestic issues." The complaining student was identified by name,[1] and the other student was identified as movant Riccardo F. Calixte.

1 Though the affidavit is filed with the Court and unsealed, we refer only generally to this student as "the student," who is also the complaining witness in the email transmission incident that is the subject of the warrant and an informant upon whom Christopher relies to establish probable cause. We do so in the interests of respecting this student's privacy.

Christopher was familiar with the reporting student because he had been a reliable witness in another unnamed investigation (of unknown outcome) that he brought to the Boston College Police Department's attention. The day after the "domestic issues" incident (January 28, 2009), Christopher met with the student, who informed the officer of the following:

- According to the student, Mr. Calixte is a computer science major who is considered a "master of the trade amongst his peers." He is also employed by the Boston College I.T. department.

- The student claimed that Mr. Calixte had a "reputation" as a "hacker."

- The student stated that it was not uncommon for Mr. Calixte to appear with unknown laptop computers which he says are given to him by Boston College for field testing or that he was fixing for other students.

- The student stated that Mr. Calixte uses two different operating systems, allegedly "to hide his illegal activities." According to the student, "[o]ne is the regular B.C. operating system and the other is a black screen with white font which he uses prompt commands on." The student also reported that Mr. Calixte's computer "has three log on fields" and that Mr. Calixte uses the nicknames "enigma" and "Bootleg enigma".

- The student claimed that he had at some unspecified time and place observed Mr. Calixte "hack into the B.C. grading system that is used by professors to change grades for students."

- The student claimed that Mr. Calixte has "'fixed' computers so that they cannot be scanned by any system for detection of illegal downloads and illegal internet use."

- The student claimed that Mr. Calixte had "jail broken" cell phones, "possibly stolen ones," so that the phones' owners could be used on other networks.

- The student claimed that Mr. Calixte had downloaded software for free, allegedly "against the licensing agreement."

- The student claimed that Mr. Calixte had "illegally downloaded movies as well as music" on his computer.

- The student claimed that Mr. Calixte had "personally implicated himself in illegal activity."

- The student also said that he suspected that Mr. Calixte was somehow causing the student's computer to "crash," though several experts looked at the machine and none of them could resolve the problem.

(Kessel Decl. Ex. A at 4-5.) Christopher also stated that Mr. Calixte was a suspect in a stolen Boston College laptop computer at some unspecified time.

In early March, the same student who had been involved in the "domestic issues" incident was the subject of a mass email to the Boston College community in which he was reported to be gay and coming out of the closet. A profile from a gay-oriented website ("adam4adam.com") including a photograph of the student was attached to the emails. The emails were sent from Google's gmail service and Yahoo! mail to a Boston College email list (or "list server"). The student suffered stress due to these emails, so a non-police Administrator asked Boston College Director of Security David Escalante to try to find out who sent the emails. Mr. Escalante advised the Detective that he traced the emails back to Calixte.[2]

From this information, Christopher apparently concluded that he had probable cause that Mr. Calixte had committed the crimes of obtaining computer services by fraud or misrepresentation under Massachusetts General Law, Chapter 266, Section 120F and unauthorized access to a computer system under Massachusetts General Law, Chapter 266, Section 33A.[3]

III. ARGUMENT

Every day that Mr. Calixte's property is in the hands of officers, he suffers irreparable harm to his property interests, privacy, and constitutional rights. *See Wright & Miller*, 11 Federal Practice & Procedure § 2948 ("When an alleged deprivation of a constitutional right is involved, most courts hold that no further showing of irreparable injury is necessary.") The warrant authorizing the seizure was not based on probable cause. He stands accused of fraud, though no

---

2 For the purposes of this emergency motion it is immaterial whether this is indeed what Mr. Escalante said, how Mr. Escalante reached this conclusion, or if there was reason to believe he was correct, since the affidavit fails to establish probable cause that sending this email is a criminal offense. Therefore, at this time Mr. Calixte does not challenge the veracity of Mr. Escalante's conclusion or the investigative activities underlying it, but does not waive his right to do so if he is ever charged with an offense.

3 Christopher erroneously cited the same section (Ch. 266 § 120F) twice, but based on his description of the two alleged offenses, it appears he intended to cite section 120F and section 33A.

money or thing of value is at issue. He is accused of "hacking" merely by sending an email to a list server. Without a crime, there is no just cause for the search. Still, Mr. Calixte has been suspended from his employment, by which he funds his education. His laptop and other materials he needs to conduct his schoolwork have been seized, so he has great difficulty completing his assignments. His cell phone has been taken so he cannot easily communicate with friends, family, or attorneys. His private communications and papers are in the hands of officers who, without just cause, continue to search for evidence of unspecified infractions or offenses. No evidence about the email could conceivably have been stored on Mr. Calixte's cell phone or iPod, and yet neither has been returned after nearly two weeks. This scope of the seizure supports the inevitable conclusion that this investigation is a fishing expedition against a student whose reputation and indeed entire educational career has suffered at the hands of a former roommate who has painted an unflattering portrait of him to school officials.

A. The Affidavit Fails to Establish Probable Cause that Any Crime Was Committed.

A search warrant may issue only on a showing of probable cause. *Commonwealth v. Byfield*, 413 Mass. 426, 428 (1992). An affidavit supporting a search warrant must contain sufficient information for an issuing magistrate to determine that the items sought are related to the criminal activity under investigation, and that the items reasonably may be expected to be located in the place to be searched at the time the warrant issues. *Commonwealth v. Rodriguez*, 49 Mass. App. Ct. 664, 667 (2000). An inference drawn from the affidavit, "if not forbidden by some rule of law, need only be reasonable and possible; it need not be necessary or inescapable." *Commonwealth v. Beckett*, 373 Mass. 329, 341 (1977). On the other hand, "[s]trong reason to suspect is not adequate." *Commonwealth v. Upton*, 394 Mass. 363, 375 (1985). It is axiomatic that the affidavit supporting a search warrant must establish probable cause that a crime has been committed. *Commonwealth v. Wade*, 64 Mass. App. Ct. 648, 651 (2005) (magistrate must have a substantial basis to conclude that a crime had been committed.)

The affidavit does not establish probable cause that any crime has been committed. Specifically, Christopher states that there is probable cause to believe that Ch. 266, sections 120F and 33A were violated. (*See* Kessel Decl. Ex. A ¶ 4(h), p. 8.) The affidavit does not provide any level of proof that those crimes were committed.

B. Sending an Email Does Not Violate Massachusetts Law.

The affidavit does not identify which of movant's alleged activities constitute the offense under investigation. However, Boston College Police derive their legal authority from Chapter 22C, Section 63, of the Massachusetts General Laws. The officers enforce local, state and federal law on the lands and structures owned, used, or occupied by the University. They are also deputized sheriffs of Middlesex and Suffolk Counties, to allow them to deal with off-campus situations, as needed. *See* http://www.bc.edu/offices/bcpd/about/powers.html (accessed Apr. 10, 2009). Their primary function is as law enforcement within the Boston College community. Therefore, the alleged offense must be the early March use of a Boston College list server to transmit an email reporting that a particular student is gay and coming out of the closet. Yet, sending such an email cannot violate sections 33A or 120F of Chapter 266.

1. There Are No Facts Establishing Probable Cause that a Commercial Computer Service Was Defrauded.

Chapter 266, Section 33A reads:

> Whoever, with intent to defraud, obtains, or attempts to obtain, or aids or abets another in obtaining, any commercial computer service by false representation, false statement, unauthorized charging to the account of another, by installing or tampering with any facilities or equipment or by any other means, shall be punished by imprisonment in the house of correction for not more than two and one-half years or by a fine of not more than three thousand dollars, or both. As used in this section, the words "commercial computer service" shall mean the use of computers, computer systems, computer programs or computer networks, or the access to or copying of the data, where such use, access or copying is offered by the proprietor or operator of the computer, system, program, network or data to others on a subscription or other basis for monetary consideration.

There are no facts establishing probable cause that a commercial computer service as defrauded. No commercial computer service is the subject of this investigation. The affidavit does not identify what commercial computer service is at issue, but none of the computers

identified is commercial. The Boston College list server, being for student use, is almost certainly not offered on a subscription basis for monetary consideration. Nor is there any statement to that effect in the affidavit. Nor is there any indication that Google or Yahoo!, both based in California, have complained about any use of their services. Both those email services are offered free of charge to the public, and are not commercial services under this statute. Yahoo! mail is generally free. *See* http://billing.mail.yahoo.com/bm/MailReg (accessed Apr. 10, 2009). So is gmail. *See* http://mail.google.com/mail/help/intl/en/about.html (accessed Apr. 10, 2009). The adam4adam.com service is also outside of Boston College Police jurisdiction, as it based in Canada. *See* http://www.adam4adam.com/?section=20&view[20]=6 (accessed Apr. 10, 2009). It is also offered at no charge. *See* http://www.adam4adam.com/ ("Join Free") (accessed Apr. 10, 2009). Thus, the affidavit fails to identify any commercial service that could be the subject of a fraud. There are no inferences that could reasonably be drawn from the facts in the affidavit from which one could conclude that a commercial service was involved in any way. It is simply impossible that sending the email in question violated this statute, patently unreasonable for the detective to have said so and for the magistrate-clerk to have issued the warrant on this basis.

2. There Are No Facts Establishing Unauthorized Access to a Computer System.

Nor does the affidavit establish probable cause under section 120F. Chapter 266 Section 120F reads:

> Whoever, 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, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both.
>
> The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.

There are no facts establishing an unauthorized access to a computer system. The allegation that someone sent this email through the Boston College list server does not demonstrate probable cause that that the transmission was unauthorized. A list server typically

refers to four things: a list of email addresses, the people ("subscribers") receiving mail at those addresses, the publications (email messages) sent to those addresses, and a reflector, which is a single email address that, when designated as the recipient of a message, will send a copy of that message to all of the subscribers. *See, e.g.,* http://en.wikipedia.org/wiki/List_server (accessed Apr. 10, 2009). List servers are extremely common and there is nothing criminal about their use. The affidavit does not state that the list server required a password or any other authentication to send email through it, or was otherwise closed to Mr. Calixte (or anyone else in the world) in any way. Thus, the affidavit gives no cause to believe that use of the list server was unauthorized.

The Commonwealth may argue that the use of this particular list server to send this particular message was "unauthorized" because it was offensive to the complaining witness, or for some reason not contained in the warrant. Any such argument must fail. After-the-fact explanations cannot remedy the issuance of a warrant based on an affidavit that is insufficient on its face. *Commonwealth v. O'Day*, 440 Mass. 296, 297 (2003) ("[O]ur inquiry as to the sufficiency of the search warrant application always begins and ends with the 'four corners of the affidavit.'")

Further, if one has authority to access a computer system, subsequent use of that system in an unanticipated or undesired way, even to send a distasteful email, does not transform the authorized access into criminal behavior. The affidavit here does not establish the nature or purpose of the list server, whether students like Mr. Calixte or indeed Mr. Calixte himself were authorized to send messages through it, whether there was any limitation on the use of the list server, or any other reason that the email transmission would have been unauthorized. Massachusetts defines "unauthorized access" as access in the face of actual notice to the user that the computer system is off-limits. In *Commonwealth v. Farley*, 1996 WL 1186936, *2-3 (Mass. Super. October 18, 1996), the Court upheld section 120F against a vagueness challenge because the statute specifically states that a password protected system gives notice that access is limited to authorized users, and the defendant had in fact used an unauthorized password. In *Commonwealth v. Piersall*, 67 Mass. App. Ct. 246, 247 (2006), the court noted that each

unauthorized "login" to a computer system constitutes a separate offense under Mass. Gen. L. ch. 266 § 120F, and defined "login" by reference to the statutory language of using a "password or other authentication to gain access" to a computer system. In that case, the evidence showed that the defendant accessed his ex-wife's email using her password. There are no facts in the affidavit from which one could infer that the list server was limited to certain users by requiring a password or some other authentication mechanism.

Section 33A was not violated by whoever transmitted the email(s) in question because no commercial services are involved. And while there are some circumstances under which a magistrate could find probable cause that unlawful computer access constitutes a misdemeanor under section 120F (*i.e.*, that there was a password or other security measure circumvented) those facts are completed absent from the affidavit. Thus, there is no probable cause to believe that a crime occurred.

C. There Is No Probable Cause to Believe that Mr. Calixte Committed Any Other Crime.

The affidavit must state precisely what crime is under investigation and establish probable cause that ***that*** crime was committed, and show that evidence of that crime is likely to be found in the place to be searched. None of the other aspersions in the affidavit even come close to meeting this standard. The affidavit contains multiple other cursory accusations against Mr. Calixte, none of which could form the basis for probable cause. Christopher says that Mr. Calixte was a suspect in a stolen laptop case he investigated, but does not say when the laptop was stolen, from whom, when the investigation commenced, what led the officer to believe that Mr. Calixte may have been involved, whether Mr. Calixte was found to have stolen the laptop, whether he was cleared, whether another person was found to be responsible, whether the investigation is ongoing, or what the nexus would be between the theft and Mr. Calixte's dorm room. The cursory statement that Mr. Calixte was a suspect doesn't even come close to probable cause to search.

Every other allegation against Mr. Calixte is made by the complaining student. These allegations fail to provide probable cause because (1) the claims do not constitute criminal offenses and/or (2) the affidavit does not demonstrate the complaining student's veracity or basis of knowledge.

1. The Remaining Allegations Against Mr. Calixte Are Not Criminal Acts.

Mr. Calixte's former roommate's allegations include that Mr. Calixte is considered a "master of the trade" at computer science, uses two operating systems, has a reputation as a "hacker," field tests or "fixes" computer for other students, uses nicknames, hacked into the college grading system to change grades for students, alters computers so they can not be scanned for detection of illegal downloads or internet use, "jailbreaks" other people's cell phones ("possibly stolen ones"), has downloaded software in violation of a licensing agreement, possesses illegally downloaded movies, and implicated himself in unspecified illegal activity on unspecified occasions.[4] Of all these allegations, only changing grades could conceivably violate the statutes Christopher cites in the affidavit. Using two operating systems is not suspicious, especially when one is a computer science major. Nor is using an operating system that has a "black screen with white font" suspicious or illegal. There is no indication of how the use of two operating systems could possibly hide illegal behavior, nor what that behavior might entail. Under certain specified circumstances, copyright infringement can be a criminal act, but the affidavit sets forth no facts from which a Court could conclude that those acts occurred here.[5] The affidavit thus lacks any allegations from which a Court could infer probable cause of criminal activity.

[4] Christopher's apparent failure to ask Boston College IT, Mr. Calixte's employer, whether or not it asked Mr. Calixte to field test computers, belies the cursory nature of Christopher's investigation and allegations.

[5] Moreover, copyright claims are subject to exclusive federal jurisdiction. *See* 28 U.S.C. 1338(a), 17 U.S.C. 506(a) (providing federal courts with exclusive jurisdiction over cases "arising under" the copyright or patent laws)

2. There Is No Probable Cause to Credit Any of the Complaining Witness' Allegations Because the Affidavit Demonstrates Neither His Reliability Nor His Basis of Knowledge.

The student informant's statements cannot be the basis for probable cause because Christopher provided no facts demonstrating that the informant is truthful, reliable, and was in a position to know what he was talking about. The affidavit relies on statements by a named informant who is also the alleged victim in this case. Statements of an informant provide the basis for probable cause only when the affidavit provides the court with "some of the underlying circumstances" regarding both the informant's reliability (the "veracity test") and the basis of his or her information (the "basis of knowledge test"). *Commonwealth v. Crawford*, 417 Mass. 40, 43 (1994), citing *Commonwealth v. Upton*, 394 Mass. 363, 375 (1985). Here, the affidavit demonstrates neither veracity nor basis of knowledge. Rather, it shows that the informant carries a grudge against Calixte, cannot discern the difference between legal and illegal use of computers, and operates based on rumors and reputation. Whatever information the informant provided was cursory, unsubstantiated, and stale. For these reasons, none of his claims, alone or together, provide probable cause.

a. Reliability

The fact that the informant was reliable once in the past falls far short of what the affiant would need to give this Court for it to find probable cause. Although past information provided by a confidential informant can establish reliability in some circumstances, *see e.g. Commonwealth* v. *Perez-Baez*, 410 Mass. 43 (1991), the past information and the manner in which the information was verified must be sufficiently detailed so that the Court can "make a meaningful determination of the informant's veracity," *Commonwealth v. Rojas*, 403 Mass. 483, 486 (1988). Courts have repeatedly held that a "naked assertion" that an informant has provided information in the past that has led to an arrest is insufficient to establish reliability. *See Rojas* at 486 (drug case); *Commonwealth v. Santana*, 411 Mass. 661, 663-665 (1992) (recital that informant had previously provided information that led to two drug-related arrests, without more, did not satisfy the veracity test); *Commonwealth v. Mejia*, 411 Mass. 108 (1991) (assertion that

confidential informant provided information leading to arrest of three named persons insufficient). Here, the affidavit merely says that the informant is "a reliable witness in another investigation which he brought to our attention." The affidavit does not identify the information given, why it was reliable, the nature of that investigation, whether it led to an arrest, nor any other facts from which a court could conclude that the information was reliable. The "naked assertions" in *Rojas*, *Santana*, and *Mejia* at least identified the type of offense and that the information led to an arrest. The statement here falls far short even of the allegations rejected as ***insufficient*** in those cases.

Other than Christopher's assertion that the confidential informant had provided reliable information in the past, there was no other reason to find the informant reliable. *Cf. Commonwealth v. Alvarez*, 422 Mass. 198 (1996) (informant considered reliable because he provided statements against his penal interest); *Commonwealth v. Fleming*, 37 Mass. App. Ct. 927, 928 (1994) (reliability of known informant established in part by his participation in a drug buy). To the contrary, the affidavit sets forth facts from which the court could infer that the informant is unreliable and has an ax to grind. The informant and Mr. Calixte used to be friends and roommates, but "were having domestic issues." The informant suspects Calixte is responsible for his computer problems. Clearly the informant thinks that Mr. Calixte was behind the transmission of the email. He wanted the officer to investigate to ***further his own interests*** against Mr. Calixte.

b. Basis of Knowledge

Nor does the affidavit establish the informant's basis for his allegations. An informant's description of the criminal activity must be sufficiently detailed, either as to what the activity is, or how the informant knows, that it raises the statement beyond rumor or reflection on reputation to probable cause. In *Commonwealth v. Alvarez*, 422 Mass. 198, 207 (1996), the promptness of the information, the specificity of the observations, and the particularity of the detail as to location permitted the inference that the informant saw the drugs at the precise place stated or saw them being carried into the apartment. In *Commonwealth v. Atchue*, 393 Mass. 343, 348

(1984), the informant claimed first-hand knowledge and gave specific descriptions of weapons he said were kept in a particular storage locker. In contrast, in *Commonwealth v. Kaufman*, 381 Mass. 301, 302-03 (1980), one informant reported that the defendant was dealing large quantities of marijuana and cocaine in the Amherst area. The other informant said that the defendant was selling marijuana and cocaine, and used a particular alias. The informants' accounts were barren of elements that could lend themselves to impressive corroboration. Rather, the statements "lacked detail, either as to its content or the process by which the content was obtained, that could raise it above the level of a casual rumor or a mere reflection of the reputation of the supposed actor." *Id., citing Spinelli v. United States*, 393 U.S. 410 (1969); *Commonwealth v. Stevens*, 362 Mass. 24, 28-29 (1972). *See Commonwealth v. Bottari*, 395 Mass. 777 (1985); *see also Commonwealth v. Brown*, 31 Mass. App. Ct. 574 (1991).

Here, the affidavit provides no facts from which a court could conclude that the informant was reporting anything beyond rumor, reflection on reputation, or mistake. The informant said that he was aware of Mr. Calixte's reputation as a "hacker" and that others considered him a "master of the trade" in computer science. He described Mr. Calixte's Dell computer, something anyone who had lived with him or visited his dorm room would have known. Like the unimpressive informants in *Kaufman*, he reported Mr. Calixte used an alias. He made some nonsensical statements asserting that using two operating systems somehow would hide illegal activities, but he was unable to identify by name either of the operating systems, saying only that one was "regular" and the other was black and white. The informant's plain ignorance shows he has no basis of knowledge for any of his claims of "hacking."

The only allegation that the informant reports on personal knowledge was that Mr. Calixte altered another student's grades. However, the informant provided no information about the date this occurred, where it happened, whether Mr. Calixte was in his dorm room, who the other student was, whether Mr. Calixte's used his own computer, the other student's machine, or some other computer entirely, or any other information one would think that a witness to such an event would have provided. In the unpublished case of *Commonwealth v. Littig*, 20 Mass. L.

Rptr. 124 (Mass. Super. 2005), the court held that statements that the informant "knows the source of the cocaine is the defendant" and that she "has met the defendant personally and knows he sells cocaine" did not suffice. "These statements provide nothing to indicate how [the informant] knows, in what context she has met him, what she has observed him doing, or what she has heard him say." *Id*. at *4. Thus the affidavit failed to establish the informant's basis of knowledge.

There are no corroborating facts from which a court could infer probable cause that Mr. Calixte changed grades. A tip in itself inadequate may be fortified through corroboration of its elements by means of police investigation. *Commonwealth v. Kaufman*, 381 Mass. 301, 303 (1980). However, no such corroboration occurred here. Since there is no probable cause to believe this incident occurred, it cannot provide the basis for the warrant.

3. There Is No Nexus Between the Informant's Allegations and Mr. Calixte's Dormitory Room.

The affidavit supporting a search warrant request must demonstrate that there is probable cause to believe that contraband will be found at the location to be searched. *Commonwealth v. Cinelli*, 389 Mass. 197, 213 (1983); *Commonwealth v. Chongarlides*, 52 Mass. App. Ct. 366, 370 (2001); *Commonwealth v. Smith*, 57 Mass. App. Ct. 907, 908 (2003). "The information in the affidavit must be adequate to establish a ***timely nexus*** between the defendant and the location to be searched and to permit a determination that the particular items of criminal activity sought can reasonably be expected to be found there." *Commonwealth v. Wade*, 64 Mass. App. Ct. 648 (2005) (emphasis added). In determining whether such a nexus exists, the court is limited to a consideration of the facts contained within the four corners of the affidavit as well as those reasonable inferences that may be drawn from the sworn information. *Chongarlides*, 52 Mass. App. Ct. at 370.

The student informant reported on January 27th and 28th, 2009 that at some unknown point in the past he had seen Mr. Calixte change another student's grade. The affidavit does not

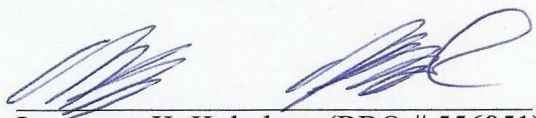
say how long in the past the event occurred. Nor does it say where the event occurred, whether it occurred in Mr. Calixte's dorm room, or whether Mr. Calixte used his own computer or another's to do the deed. On March 30, 2009, Christopher applied for the warrant to search Mr. Calixte's room. There was no reason to believe that any evidence of grade changing still existed, since it had happened somewhere between two months and several years in the past.

Second, there was no nexus between the alleged activity and Mr. Calixte's dorm room. In *Commonwealth v. Smith*, 57 Mass. App. Ct. 907 (2003), the court found no probable cause to search the defendant's residence. There, the defendant was on one occasion seen returning to his residence after a drug sale to a confidential informant, and on another occasion seen leaving his residence to make a sale to an undercover officer. *Smith*, 57 Mass. App. Ct. at 907. In finding that the affidavit failed to establish a proper nexus, the *Smith* court emphasized the fact that the confidential informant had never claimed to be inside the defendant's residence and had never claimed that the defendant conducted drug transactions from his residence or kept drug related items there. Here, the informant provided even less information than in *Smith.* As in that case, there is no nexus between Mr. Calixte's room and any alleged grade changing offense.

IV. CONCLUSION

For all these reasons, the search warrant is invalid. The March 30th search and seizure were illegal, and the ongoing retention and analysis of Mr. Calixte's property, computers, and data violate his state and federal constitutional rights. This harm is irreparable. Therefore, this Court should issue emergency relief by (1) quashing the warrant (2) ordering officers to cease searching and analysis the items seized (3) order the return of all property and data seized and (4) order that any stored copies of Mr. Calixte's data be deleted.

Riccardo Calixte
By His Attorneys:



Lawrence K. Kolodney (BBO # 556851)
Email: kolodney@fr.com
Adam J. Kessel (BBO # 661211)
Email: kessel@fr.com
Thomas A. Brown (BBO # 657715)
Email: tbrown@fr.com
FISH & RICHARDSON P.C.
225 Franklin Street
Boston, MA 02110-2804
(617) 542-5070 (Telephone)
(617) 542-8906 (Facsimile)

Of Counsel

Jennifer Stisa Granick, CA Bar No. 168423
Email: jennifer@eff.org
Matt Zimmerman, CA Bar No. 212423
Email: mattz@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333

Dated: April 10, 2009