Jennifer Stisa Granick, Esq. (SBN 168423)
Matthew Zimmerman, Esq. (SBN 212423)
Marcia Hofmann, Esq. (SBN 250087)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: jennifer@granick.com
mattz@eff.org
marcia@eff.org

Michael T. Risher (SBN 191627)
AMERICAN CIVIL LIBERTIES FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, California 94111
Telephone: (415) 621-2493
Facsimile: (415) 255-8437
Email: mrisher@aclunc.org

Attorneys for Plaintiffs
LONG HAUL, INC. and EAST BAY PRISONER SUPPORT

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

LONG HAUL, INC. and EAST BAY PRISONER SUPPORT, Plaintiffs, v. UNITED STATES OF AMERICA; MITCHELL CELAYA; KAREN ALBERTS; WILLIAM KASISKE; WADE MACADAM; TIMOTHY J. ZUNIGA; MIKE HART; LISA SHAFFER; AND DOES 1-25, Defendants.	Case No. C 09-00168-JSW PLAINTIFFS' NOTICE OF MOTION AND MOTION FOR SUMMARY JUDGMENT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT Date: April 8, 2011 Time: 9:00 AM Dept.: 11

TO DEFENDANTS AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that at 9:00 am on April 8, 2011, or as soon thereafter as the matter may be heard in Courtroom 11 on the 19th Floor of the United States District Court for the Northern District of California, 450 Golden Gate Avenue, San Francisco, California, Plaintiffs Long Haul, Inc. ("Long Haul") and the East Bay Prisoner Support ("EBPS") will, and hereby do, move for summary judgment against all Defendants.

Pursuant to Federal Rule of Civil Procedure 56, Plaintiffs seek a declaration that Defendants Karen Alberts, William Kasiske, Wade MacAdam, Timothy J. Zuniga, Mike Hart, and Lisa Shaffer violated the Fourth Amendment to the United States Constitution in searching Plaintiffs' property, and seizing materials during that search, on August 28, 2008; that Defendants United States and Kasiske are liable for the overbroad forensic search conducted on seized digital data; and that Defendant Mitchell Celaya is liable for the acts of the UC Defendants in his official capacity. Plaintiffs also seek an order declaring that Defendants are liable for violating the Privacy Protection Act, 42 U.S.C. §§ 2000aa (2006), *et seq*., by searching and seizing Plaintiffs' physical and electronic documents covered by the Act. This Motion is based on this Notice of Motion; the Memorandum of Points and Authorities in support of this Motion; the Declarations of Matthew Zimmerman, Patrick Lyons, Jesse Palmer, and Kathryn Miller in support of this Motion; all papers and records on file with the Clerk or which may be submitted prior to or at the time of the hearing; and any further evidence and argument which may be offered.

DATED: January 31, 2011

By */s/ Jennifer Stisa Granick*
JENNIFER STISA GRANICK

c/o ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x127
Facsimile: (415) 436-9993

COUNSEL FOR PLAINTIFFS

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTRODUCTION 1

STATEMENT OF FACTS 1

LEGAL STANDARD 9

ARGUMENT 10

I. DEFENDANTS VIOLATED THE FOURTH AMENDMENT 10

A. The Search Warrant Was Unconstitutionally Overbroad 10

1. The Warrant Authorized a Search for the Identity of Long Haul Computer Patrons Without Limitation as to Date or Time 12

2. The Warrant Authorized the Seizure of All Storage Media, Regardless of Whether Computer Logs Were Likely to Be Stored There 13

3. The Warrant Authorized a Search "For Evidence" Without Limitation. 14

B. The Statement of Probable Cause Cannot Cure the Warrant's Facial Overbreadth. 15

1. The Statement of Probable Cause Was Not Present at Long Haul During the Search. 15

2. The Raid Team's Conduct During the Search Itself Was Unreasonably Intrusive. 16

II. DEFENDANTS VIOLATED THE PRIVACY PROTECTION ACT 18

A. Defendants Seized Work Product Materials in Violation of the PPA. 19

B. Defendants Seized Documentary Materials in Violation of the PPA. 22

III. Each Raid Team Defendant Is Individually Liable as an Integral Participant in the Unlawful Search. 23

IV. CONCLUSION 25

TABLE OF AUTHORITIES

Cases

Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) 10, 23

Blankenhorn v. City of Orange, 485 F.3d 463 (9th Cir. 2007) 24

Boyd v. Benton County, 374 F.3d 773 (9th Cir. 2004) 23, 24, 25

Chuman v. Wright, 76 F.3d 292 (9th Cir. 1996) 24

Coolidge v. New Hampshire, 403 U.S. 443 (1971) 10

Groh v. Ramirez, 540, U.S. 551 (2004) 15, 23

James v. Sadler, 909 F.2d 834 (5th Cir. 1990) 25

Jones v. Williams, 297 F.3d 930 (9th Cir. 2002) 25

Maryland v. Garrison, 480 U.S. 79 (1987) 22

Melear v. Spears, 862 F.2d 1177 (5th Cir. 1989) 23, 24, 25

Mena v. City of Simi Valley, 226 F.3d 1031 (9th Cir. 2000) 17

Millender v. County of Los Angeles, 620 F.3d 1016 (9th Cir. 2010) (*en banc*) ..... passim

Motley v. Parks, 432 F.3d 1072 (9th Cir. 2005) 21, 22, 23

United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006) 11

United States v. Cardwell, 680 F.2d 75 (9th Cir. 1982) 14

United States v. Comprehensive Drug Testing, 621 F.3d 1162 (9th Cir. 2010) 18

United States v. Giberson, 527 F.3d 882 (9th Cir. 2008) 17

United States v. Hill, 459 F.3d 966 (9th Cir. 2006) 11, 18

United States v. Kow, 58 F.3d 423 (9th Cir. 1995) 15

United States v. Payton, 573 F.3d 859 (9th Cir. 2009) 11, 17

United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) 11

United States v. SDI Future Health, 568 F.3d 684 (9th Cir. 2009) 13

United States v. Spilotro, 800 F.2d 959 (9th Cir.1986) ..... passim

United States v. Stubbs, 873 F.2d 210 (9th Cir. 1989) 13

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982) 18

United States v. Washington, 797 F.2d 1461 (9th Cir. 1986) 14

Zurcher v. Stanford Daily, 436 U.S. 547 (1978) 19, 24

Statutes and Legislative Authorities

26 U.S.C. § 7201 15

42 U.S.C. § 1983 (2006) 10, 23, 24

Fed. R. Civ. P. 56(c) 9

Privacy Protection Act, 42 U.S.C. § 2000aa (2006), *et seq*. ..... passim

S. Rep. 96-874 (1980) 19

U.S.C.C.A.N. 3950 (1980) 19

INTRODUCTION

Plaintiff Long Haul is an all-volunteer collective that provides a lending library, a bookstore, Internet-connected computers, and a community space to members of the public. Long Haul also publishes Slingshot, a quarterly newspaper, out of an office on its second floor. Plaintiff East Bay Prisoner Support ("EBPS") is a separate organization devoted to prison reform that rents office space on the Long Haul premises.

Defendant state and federal law enforcement agents violated the Fourth Amendment by (among other actions) obtaining and executing a facially overbroad warrant, and by searching outside the scope of probable cause offered in support of the warrant, which was that an unknown patron had used one of the Long Haul's public-access computers to send threatening emails on specific dates in March and June of that year. Defendants also violated the Privacy Protection Act ("PPA," 42 U.S.C. § 2000aa (2006), *et seq*.) by searching and seizing computers and digital files belonging to the Slingshot newspaper and to EBPS which contained both "documentary" and "work product" materials protected under the PPA.

STATEMENT OF FACTS

Long Haul was founded as an unincorporated association in 1979 by Alan Haber, one of the founding members of the 1960s new-left group Students for a Democratic Society. Declaration of Jesse Palmer ("Palmer Decl.") ¶ 2. It is an all-volunteer collective that educates the public about peace and justice and serves as a meeting space for activist groups, radical movie nights, anarchist study groups, and other community meetings and events. *Id.* The organization has long been housed at a two-story storefront at 3124 Shattuck Avenue, in Berkeley. Declaration of Matthew Zimmerman ("Zimm. Decl.") Ex. 4 (Palmer Dep. Vol. 1 ("*Palmer 1*")) 19:17-18. Long Haul is well known, if not well liked,[1] by University of California law enforcement as a place where activists

[1] Defendant Kasiske, upon tracing the email messages being investigated back to an IP address associated with a Long Haul Internet account, told his supervisor that it was "no surprise" that the messages went back to the Infoshop, and suggested that Long Haul would not assist in an investigation into the identity of the individual(s) who sent the emails. Zimm. Decl. Ex. 6 (Kasiske Dep. ("*Kasiske*")) 86:4-87:8. Similarly, Defendant Celaya told a local news reporter that Long Haul could not be trusted to respond to a subpoena because "Some people are not ethical or moral in helping to solve a crime." *See* video at http://www.youtube.com/watch?v=FbS_K89-SXI (last accessed on January 30, 2011).

meet. Zimm. Decl. Ex. 3 (Statement of Probable Cause) at 2 (Defendant Kasiske stating "I know that the Long Haul is a resource and meeting center for radical activists. I know that animal rights activists have held meetings at the Long Haul."); Zimm. Decl. Ex. 7 (Zuniga Dep. ("*Zuniga*")) 20:6-14, 26:9-11 (Defendant Zuniga looked at the Long Haul website prior to the raid); Zimm. Decl. Ex. 8 (Shaffer Dep. ("*Shaffer*")) 23:3-17; Zimm. Decl. Ex. 9 (Shaffer's Resp. to Pl.'s First Set of Interrogs. # 10) (Defendant Shaffer was aware that activists would go to Long Haul for meetings, discussions).

A private office, located in a separate loft with its own staircase at the Long Haul premises, houses Slingshot, a newspaper with both print and online distribution. Palmer Decl. ¶ 3. Slingshot is frequently critical of the University, University of California Police Department ("UCPD") officers, and practices. Palmer Decl. ¶ 4. Slingshot began publication in 1988 and was subsequently moved from the UC Berkeley campus to its current location in 1993. Zimm. Decl. Ex. 4 (*Palmer 1*) 77:21-79:1. Print editions of Slingshot published since April 1994 indicate that Slingshot is published out of Long Haul. Palmer Decl. ¶ 5. Moreover, at the time of the raid, the Slingshot web site (located at http://slingshot.tao.ca) indicated that the Slingshot publication was published out of Long Haul. Palmer Decl. ¶ 12; Palmer Decl. Exs. 2, 3 (copies of Slingshot web site pages). There were approximately 16,000 copies of the Spring 2008 issue of Slingshot (i.e., the issue prior to the raid) printed and distributed. Palmer Decl. ¶ 6. UC Berkeley Police officers had long been generally familiar with Slingshot. Palmer Decl. ¶ 16; Palmer Decl. Ex. 7 (published photo of UC Berkeley police officers reading Slingshot).

At the time of the search in question, a sign reading "Slingshot" hung over the entrance to the Slingshot office. Palmer Decl. ¶ 3; Palmer Decl. Ex. 8. The office also contained an archive of back issues of the newspaper. Zimm. Decl. Ex. 8 (*Shaffer*) 59:17-61:5 (archival copies of publications on a shelf in the office). The office further contained computers that were used to publish the newspaper. Zimm. Decl. Ex. 5 (Palmer Dep. vol. 2 ("*Palmer 2*")) 301:23-302:6, 325:11-14. These computers contained a large amount of unpublished material relating to Slingshot, including hundreds of drafts of articles and articles that had been submitted but never published, as well as archival versions of the newspaper. Zimm. Decl. Ex. 5 (*Palmer 2*) 306:13-24, 377:21-378:3; Zimm.

Decl. Ex. 10 (Miller Dep. ("*Miller*")) 48:14-49:22; Palmer Decl. ¶ 21; Palmer Decl. Exs. 12-15 (sample documents from the seized Slingshot computers).

Long Haul rents office space to other organizations. Zimm. Decl. Ex. 4 (*Palmer 1*) 71:21-23. At the time of the search that is the subject of this lawsuit, Plaintiff EBPS had an office at Long Haul, as did Cycles of Change and the Needle Exchange. Zimm. Decl. Ex. 4 (*Palmer 1*) 90:19-21, 25:2-26:3; Zimm. Decl. Ex. 11 (Lyons Dep. ("*Lyons*")) 22:22-25. These three offices were right next to each other and labeled with the names of the tenants on their respective doors. Zimm. Decl. Ex. 4 (*Palmer 1*) 63:20-25; Zimm. Decl. Ex. 11 (*Lyons*) 53:24-54:8, 55:7-11; Declaration of Patrick Lyons ("Lyons Decl.") ¶ 2; Lyons Decl. Ex. 2 (photo of EBPS door with sign).

Long Haul also offers free Internet access to the public in a labeled computer room located in an open loft area that is accessible by a single staircase, opposite to and separate from the staircase and loft area related to the (locked) Slingshot office. Zimm. Decl. Ex. 4 (*Palmer 1*) 97:1-7. This unenclosed area is not secured and is visible from the central common area below. *Id.* Long Haul did not and does not keep any records of who uses these public-access computers. Palmer Decl. ¶ 9.

According to the August 26, 2008, Statement of Probable Cause submitted to the magistrate judge by Defendant UCPD Officer William Kasiske, on two separate occasions in March and June of 2008, an unknown individual sent threatening emails to University of California ("UC") animal researchers. Following the March and June emails, Kasiske identified the Internet protocol ("IP") address of the computer that sent these threatening emails, issued a subpoena to the internet service provider that owned that IP address, and learned that, at the time the emails were sent, the IP address correlated to an Internet account tied to the Long Haul address. Kasiske noted that "Long Haul's website advertises that they offer a computer room with four computers for 'activist oriented access.'" He then stated that "establishments that offer public computer access often have some type of a system for patrons to sign in or register to use the computers," and that a search of Long Haul "could reveal logs or sign in sheets" that could help identify the suspect. Officer Kasiske also stated that the suspect might have used the computers for other purposes that could have left records that might aid in identifying the suspect. Zimm. Decl. Ex. 3 (Statement of Probable Cause).

There is no indication that Kasiske took any steps to determine whether any other IP addresses were associated with Long Haul's physical address. Zimm. Decl. Ex. 6 (*Kasiske*) 136:23-137:11. Kasiske made no effort to determine whether Long Haul in fact used a sign-in process. *Id*. 48:5-8. Nothing in the warrant or its attachments made any reference to EBPS or the two other private offices that were located at Long Haul but rented by other organizations. The Statement of Probable Cause does not contain information that any computers other than the public-access computers would be relevant to the investigation; nor does it contain information that Plaintiffs were suspected of any wrongdoing, that anyone associated with the Plaintiffs had sent the emails being investigated, or that there was reason to believe that individuals associated with Long Haul would improperly resist a subpoena or other legal process. *See also id.* 93:17-94:12 (Defendant Kasiske had not tried either using a subpoena or asking directly for information from Long Haul).

Along with this Statement of Probable Cause, Kasiske presented the judge with a pre-printed warrant form and another attachment that Kasiske drafted, which described the "places to be searched" and the "property to be seized." Zimm. Decl. Ex. 1 (search warrant and attachments). *See also* Zimm. Decl. Ex. 6 (*Kasiske*) 21:2-17, 52:18-25 (discussing Kasiske's decision to cut and paste language from a boilerplate department warrant form into his warrant application). This attachment described the places to be searched as "[t]he premises, structures, rooms, receptacles, outbuildings, associated storage areas, and safes situated at the Long Haul Infoshop, 3124 Shattuck Avenue, Berkeley, CA." Zimm. Decl. Ex. 1 (search warrant and attachments). It also described the things to be seized as all documents containing the "names or other identifying information of patrons who used the computers at Long Haul." *Id.* The descriptions did not limit investigators to the time period during which the threatening emails were sent or to evidence regarding the sender of the offending emails. The warrant also authorized the seizure of a wide range of other computer or electronic storage devices: "[a]ll electronic data processing and storage devices … and computer systems, including but not limited to central processing units, external hard drives, CDs, DVDs, diskettes, memory cards, PDAs, and USB flash drives." *Id*. The affidavit does not offer any basis for a belief that such hardware, including non-writable media devices such as music CDs and movie DVDs, might contain patron logs. *See also* Zimm. Decl. Ex. 6 (*Kasiske*) 115:13-116:13. The

attachment authorized officers to transfer all of these items to a secondary location to search them "for evidence," without any limitation or explanation as to what type of evidence was to be sought. Zimm. Decl. Ex. 3 (Statement of Probable Cause) at 4.

Kasiske signed the affidavit, incorporating his Statement of Probable Cause and the property to be searched and seized, at 11:25 AM on August 26, 2008. Five minutes later, at 11:30 AM, the magistrate signed the warrant without modification. *Id.* Defendant Kasiske sought the warrant with the knowledge and consent of his supervisors, Lt. Doug Wing and Defendant Sgt. Karen Alberts. Zimm. Decl. Ex. 6 (*Kasiske*) 69:10-13, 82:21-83:10; Zimm. Decl. Ex. 12 (Alberts Dep. (*Alberts*)) 63:22-65:13; Zimm. Decl. Ex. 13 (Celaya's Resp. to Pl.'s Req. for Admis. # 22, 23).

The next morning, the morning of the execution of the warrant (August 27, 2008), Kasiske called a meeting of the raid team, which included himself, Alberts, UCPD officers MacAdam and Zuniga, FBI Special Agent Defendant Lisa Shaffer, and retired Alameda County Officer Defendant Mike Hart, who was deputized and working for the FBI with the UC Berkeley Animal Rights Task Force at the time. Zimm. Decl. Ex. 6 (*Kasiske*) 63:9-64:20; Zimm. Decl. Ex. 14 (Strange Dep. ("*Strange*")) 9:17-11:16. During the briefing, Kasiske did not specify which areas in Long Haul's building were to be searched, that any areas were off limits, or that any portions of the building belonged to other entities. Zimm. Decl. Ex. 6 (*Kasiske*) 76:1-6; Zimm. Decl. Ex. 8 (*Shaffer*) 36:13-22. Nor did Kasiske instruct the other defendants what to do if the search revealed offices belonging to other entities. Zimm. Decl. Ex. 6 (*Kasiske*) 76:12-19; Zimm. Decl. Ex. 8 (*Shaffer*) 36:23-37:2.

After their pre-raid briefing, the raid team traveled to the Long Haul premises. Zimm. Decl. Ex. 12 (*Alberts*) 94:22-95:4; Zimm. Decl. Ex. 7 (Zuniga Dep. ("*Zuniga*")) 43:23-44:16, 45:4-22 (Zuniga arrived after initial entry). The raid team entered the Homeless Action Center next door to Long Haul, went through that office to the back of the Long Haul space, and entered Long Haul through the closed back door. Zimm. Decl. Ex. 4 (*Palmer 1*) 148:19-149:14; Zimm. Decl. Ex. 6 (*Kasiske*) 98:13-15; Zimm. Decl. Ex. 12 (*Alberts*) 96:4-12; Zimm. Decl. Ex. 15 (MacAdam Dep. ("*MacAdam*")) 45:20-22; Zimm. Decl. Ex. 8 (*Shaffer*) 49:11-23. Wearing insignia of their law enforcement capacity (such as uniforms and jackets identifying their law enforcement affiliation), and with guns drawn, the raid team entered the premises through the Long Haul back door and

performed a protective sweep (i.e., ensuring that no one was inside). Zimm. Decl. Ex. 15 (*MacAdam*) 45:5-11; Zimm. Decl. Ex. 14 (*Strange*) 36:2-9; Zimm. Decl. Ex. 6 (*Kasiske*) 100:9-11; Zimm. Decl. Ex. 8 (*Shaffer*) 50:15-21.

The raid team spent over two hours searching the premises. Zimm. Decl. Ex. 19 (UCBPD call log indicating defendants arrived at 9:52 a.m. and left at 12:14 p.m.). While inside, the raid team went through every room, both public and locked – cutting, crowbarring, or unscrewing the locks. Zimm. Decl. Ex. 6 (*Kasiske*) 109:6-19; Zimm. Decl. Ex. 14 (*MacAdam*) 50:6-9; Zimm. Decl. Ex. 16 (MacAdam Resp. to Pl.'s Req. for Admis. # 25); Zimm. Decl. Ex. 7 (*Zuniga*) 52:13-53:11; Zimm. Decl. Ex. 27. The raid team cut locks from cabinets behind the front desk, looked through the log of individuals who borrowed books from Long Haul's library, and searched Long Haul's log of book sales, both of which were stored there. Zimm. Decl. Ex. 5 (Palmer Dep. vol. 2 ("*Palmer 2*")) 313:3-317:4; Zimm. Decl. Ex. 10 (*Miller*) 74:18-22; Declaration of Kathryn Miller ("Miller Decl.") ¶ 5; Zimm. Decl. Ex. 12 (*Alberts*) 100:6-17; Zimm. Decl. Ex. 15 (*MacAdam*), 57:16-58:12; Zimm. Decl. Ex. 8 (*Shaffer*) 51:22-52:4; Zimm. Decl. Ex. 9 (Shaffer's Resp. to Pl.'s First Set of Interrogs. # 8).

The raid team removed every computer from the building. Zimm. Decl. Ex. 6 (*Kasiske*) 103:1-117:20; Zimm. Decl. Ex. 7 (*Zuniga*) 55:11-19; Zimm. Decl. Ex. 16 (Def. Hart's Resp. to Pf.'s Req. for Admis. # 12). They removed all the public-access computers from Long Haul's unmonitored public space where people come to use the machines just as they would at a public library. Zimm. Decl. Ex. 6 (*Kasiske*) 138:4-19; Zimm. Decl. Ex. 5 (*Palmer 2*) 381:21-382:2; Zimm. Decl. Ex. 18 (Harris Dep. ("*Harris*") 75:6-12. They also removed all the computers from closed, locked offices. The raid team broke open the locked, labeled door of the Slingshot office and seized the Slingshot computers, which contained hundreds of documents prepared as part of creating the newspaper (documents protected by the PPA). Zimm. Decl. Ex. 5 (*Palmer 2*) 306:13-24, 377:21-378:3; Zimm. Decl. Ex. 10 (Miller Dep. ("*Miller*")) 48:14-49:22; Palmer Decl. ¶ 21; Palmer Decl. Exs. 12-15 (sample documents from the seized Slingshot computers). *See also* Zimm. Decl. Ex. 6 (*Kasiske*) 139:24-140:10; Zimm. Decl. Ex. 7 (*Zuniga*) 55:11-19; Zimm. Decl. Ex. 8 (*Shaffer*) 66:23-67:1 (removal of computers from premises). At the time of the raid, at least Defendants Zuniga,

Alberts, and Hart knew that Slingshot was a publication and that Slingshot and Long Haul were connected. Zimm. Decl. Ex. 12 (*Alberts*) 57:5-59:21; Zimm. Decl. Ex. 28; Zimm. Decl. Ex. 7 (*Zuniga*) 29:11-30:9, 30:13-24; Zimm. Decl. Ex. 26; Zimm. Decl. Ex. 8 (*Shaffer*) 24:5-15; Zimm. Decl. Ex. 16 (Hart's Resp. to Pf.'s Req. for Admis. # 11).

Defendants Zuniga and Shaffer personally searched the Slingshot filing cabinets, including files, folders and documents stored therein. Zimm. Decl. Ex. 6 (*Kasiske*) 118:16-21; Zimm. Decl. Ex. 12 (*Alberts*) 110:16-111:24; Zimm. Decl. Ex. 7 (*Zuniga*) 55:16-56; Zimm. Decl. Ex. 8 (*Shaffer*) 56:17-57:4; 59:17-61:5; Zimm. Decl. Ex. 9 (Shaffer's Resp. to Pl.'s First Set of Interrogs. # 8). Zuniga searched through a photo archive and called Shaffer to examine more closely a photo he recognized as being taken in Seattle. Zimm. Decl. Ex. 9 (Shaffer's Resp. to Pl.'s First Set of Interrogs. # 8); Zimm. Decl. Ex. 7 (*Zuniga*) 54:15-25, 55:1-6, 63:7-64:20, 65:12-23, 66:15-25; Zimm. Decl. Ex. 8 (*Shaffer*) 55:23-56:11; Zimm. Decl. Ex. 12 (*Alberts*) 112:9-11. Seattle has no connection to the emails that the Defendants were supposed to be investigating, nor could photos contain logs of who used the public access computers. The raid team left photographs that had been archived in the filing cabinet piled on the desk in the Slingshot office. Zimm. Decl. Ex. 10 (*Miller*) 76:9-11. Officers left a humorous *circa* 1994 photo of some nude individuals in face masks on the top of the pile. Miller Decl. ¶ 8.

The raid team also entered the locked, labeled EBPS office – damaging its door in the process – and seized the EBPS computer. Zimm. Decl. Ex. 5 (*Palmer 2*) 351:10-18; Zimm. Decl. Ex. 6 (*Kasiske*) 108:13-109:19; Zimm. Decl. Ex. 8 (*Shaffer*) 62:22-63:2; Zimm. Decl. Ex. 18 (*Harris*) 70:9-13; Zimm. Decl. Ex. 11 (*Lyons*) 85:6-86:21. The EBPS computer, too, contained documentary and work-product materials as described by the PPA, including information intended for prisoners and information from prisoners intended for the general public. Lyons Decl. ¶ 3; Lyons Decl. Ex. 2 (sample documents from the seized EBPS computer). The fact that EBPS disseminated information to prisoners and other members of the public was described on the EBPS MySpace page and the Long Haul website at the time of the raid. Lyons Decl. ¶ 4; Lyons Decl. Ex. 3 (copy of EBPS MySpace page); Palmer Decl. ¶ 11; Palmer Decl. Ex. 1 (copy of Long Haul web site home page). The raid team also seized miscellaneous CDs, computer disks and a USB drive

from this office. Zimm. Decl. Ex. 18 (*Harris*) 70:22-71:17. The raid team left the EBPS office in disarray. Zimm. Decl. Ex. 18 (*Harris*) 70:20-24; Zimm. Decl. Ex. 11 (*Lyons*) 89:7-21. For example, prior to the raid, EBPS had physically organized its voluminous prisoner mail in separate, categorized piles. The raid team left the EBPS mail in one jumbled pile upon exiting the Long Haul premises after the raid. Zimm. Decl. Ex. 8 (*Shaffer*) 64:21-65:1; Zimm. Decl. Ex. 9 (Shaffer's Resp. to Pl.'s First Set of Interrogs. # 8) (describing Shaffer's search of the EBPS office); Zimm. Decl. Ex. 11 (*Lyons*) 87:15-23.

After the raid, Defendant Kasiske asked UC Berkeley employee Nicole Miller and the Silicon Valley Regional Computer Forensics Lab ("the Lab")[2] to copy the data from the computers and storage media seized from Long Haul, the Slingshot office, and the EBPS office. Zimm. Decl. Ex. 20 (Kasiske's Resp. to Pl.'s Req. for Admis. # 35). The seized devices were returned to Plaintiffs following the raid, but Defendants retained copies of the data – which they have to this day. Zimm. Decl. Ex. 11 (*Alberts*) 148:13-17, 149:8-14; Zimm. Decl. Ex. 20 (Kasiske's Resp. to Pl.'s Req. for Admis. # 35); Zimm. Decl. Ex. 16 (MacAdam Resp. to Pl.'s Req. for Admis. # 20, 21).

Kasiske then ordered a forensic examination by the Lab of six of the Long Haul public access computers. Zimm. Decl. Ex. 6 (*Kasiske*) 132:5-11. Kasiske initially asked the lab to search all the computers, even those taken from private offices. *Id*. 136:17-22. Kasiske then narrowed his search to include only the public-access computers, noting that they were the "most likely" to contain actual evidence. Zimm. Decl. Ex. 25; Zimm. Decl. Ex. 6 (*Kasiske*) 136:7-25, 138:18-19. In addition to information related to the identity of the author of the March and June emails ostensibly being searched for pursuant to the warrant, Kasiske asked the lab to search for the names of suspects in other cases. Zimm. Decl. Ex. 25 at 2. No evidence relevant to any criminal activity was found.

The raid disrupted Plaintiffs' ability to communicate with members of the public and to carry out their other operations. Zimm. Decl. Ex. 5 (*Palmer 2*) 293:10-19 (describing that the loss of Long Haul's computers meant that Long Haul's ability to communicate and organize was disrupted, and

[2] The lab is an agency of Defendant United States. Strange Dep. 72:4-8 (the United States helps to fund and organize the Lab); Zimm. Decl. Ex. 20, Beeson Dep. ("*Beeson"*) 13:17-21 (FBI is the Lab's primary funding source, and the lab follows FBI principles and protocols as they relate to computer forensic material), 14:7-12 (some employees at the Lab are employed by the FBI).

that it had to spend time replacing its computers and restoring data), 297:11-24 (discussing how the loss of Long Haul's computers resulted in its inability to schedule educational events)). Long Haul's ability to publish Slingshot was disrupted by the seizure of Slingshot computers and storage media. Palmer Decl. Exs. 4-6 (emails discussing impact of loss of computers on publication of Slingshot and urging members not to bring personal computers to Long Haul due to concerns about future seizures). EBPS's ability to provide information to the public about prisoner rights and prisoner support efforts was disrupted by the seizure of EBPS's computer and storage media. Zimm. Decl. Ex. 18 (*Harris*) 86:22-87:6 (EBPS members could not access EBPS email account after computer was taken during raid); Zimm. Decl. Ex. 11 (*Lyons*) 104:19-106:23 (raid required EBPS to spend over ten hours reorganizing office, correspondence, and fixing door; removal of computer disrupted EBPS's ability to read and send emails); 110:16-23, 114:21-115:8 (EBPS feared the FBI and police would continue to monitor their activities). Plaintiff Long Haul's ability to lend books, sell books, host gatherings, and have meetings of Long Haul members and other associates was disrupted by the search of the library lending log, the sales log, the seizure of the property and the ongoing reasonable belief that Long Haul space is, or will be, subject to further police surveillance. Zimm. Decl. Ex. 5 (*Palmer 2*) 313:13-314:12, 315:15-20, 316:20-24 (discussing how the searches of Long Haul's lending and sales records disrupted Long Haul's activities by making patrons concerned about whether their records would be searched by police), 293:1-22 (discussing how Defendants' searches and seizures of Long Haul's computers and hardware disrupted Long Haul's business by halting all work done on its computers and forcing it to spend time replacing its computers and data), 328:14-331:15 (stating that Long Haul was concerned about the possibilities or realities of police surveillance after the illegal search and seizure); Palmer Decl. Exs. 4, 5 (emails expressing concern about government monitoring).

LEGAL STANDARD

Courts must render summary judgment "if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c).

ARGUMENT

I. DEFENDANTS VIOLATED THE FOURTH AMENDMENT

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

State and federal law enforcement officers who violate the Fourth Amendment are liable to the injured parties under 42 U.S.C. § 1983 (2006) and *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 392 (1971), respectively. Defendants violated the Fourth Amendment because they acted pursuant to a facially overbroad warrant and they failed to constrain their search to places and things for which probable cause may have existed. Each raid team Defendant was personally involved in either the search or seizure of private spaces or things, and each raid team Defendant is jointly and severally liable as an integral participant in this search and seizure.[3]

A. The Search Warrant Was Unconstitutionally Overbroad.

To "prevent[] general, exploratory searches and indiscriminate rummaging through a person's belongings," the Fourth Amendment requires that warrants be specific in their description of what searches and seizures are authorized. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Thus, even "those searches deemed necessary should be as limited as possible." *Id*. To determine whether a warrant is sufficiently specific, the Court considers:

> (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued.

United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986) (Kennedy, J.); *Millender v. County of Los Angeles*, 620 F.3d 1016, 1024 (9th Cir. 2010) (*en banc*).

The first consideration embodies the "overarching Fourth Amendment principle" that police

[3] Defendant Celaya is sued in his official capacity only.

must have probable cause to search for and seize "all the items of a particular type described in the warrant." *Spilotro*, 800 F.2d at 963. The other two considerations allow the government to describe categories more broadly in two limited circumstances – if the warrant also contains language that provides sufficient guidance to the police to determine what is covered by the warrant, *id.* at 1025-26, or if the government does not have sufficient information to provide a more specific description of the items sought, *id*. at 1026-27. This is truly a rule of necessity – it cannot apply if "a more precise description of the items sought was possible." *Spilotro*, 800 F.2d at 964, 965 ("authorization to seize 'gemstones and other items of jewelry' was far too broad" when police sought only to "search the store for *stolen* gems or jewelry") (emphasis added)).

Searches of computers and data storage media present particular concerns under the Fourth Amendment because they contain so much sensitive data: "The nature of computers makes such searches so intrusive that affidavits seeking warrants for the search of computers often include a limiting search protocol, and judges issuing warrants may place conditions on the manner and extent of such searches, to protect privacy and other important constitutional interests." *United States v. Payton*, 573 F.3d 859, 864 (9th Cir. 2009) (citing *United States v. Adjani*, 452 F.3d 1140, 1149 n.7 (9th Cir. 2006)). Judicial officers must be given the option of imposing such conditions when authorizing the search of computers. *Id*. It is particularly important that a search warrant authorize only the seizure of those computers and storage media for which there is probable cause: "there must be some threshold showing before the government may 'seize the haystack to look for the needle.'" *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006). *See also Payton*, 573 F.3d at 863 (9th Cir. 2009) (where there was no reason to believe that the computer seized would have contained the sales logs identified in the warrant, seizure and search of the computer violated the Fourth Amendment); *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005) (in an investigation into harassing phone calls, a warrant authorizing seizure of all storage media and "not limited to any particular files" violated the Fourth Amendment).

A search conducted under a warrant that is partially invalid because a part of it is overbroad violates the Fourth Amendment rights of the people whose property is searched or seized at the time of the unreasonable intrusion. *Millender*, 620 F.3d at 1024.

1. The Warrant Authorized a Search for the Identity of Long Haul Computer Patrons Without Limitation as to Date or Time.

The first paragraph of the search warrant's description of "property to be seized" authorized the seizure of "[a]ny written, typed, or electronically stored documents, papers, notebooks, or logs containing names or other identifying information of patrons who used the computers at the Long Haul Infoshop." Zimm. Decl. Ex. 1. A comparison with the Ninth Circuit's recent *en banc* decision in *Millender* shows that this is facially overbroad because the warrant should have, and easily could have, limited the scope so as only to include documents and logs relating to the particular dates in March and June when the harassing emails were sent.

In *Millender*, the victim told the officers that her ex-boyfriend had shot at her with "a black sawed-off shotgun with a pistol grip" and provided a photograph of the suspect with the gun. Officers then obtained a warrant to search "for essentially any device that could fire ammunition, any ammunition, and any firearm-related materials." 620 F.3d at 1025. While officers clearly had probable cause to search the suspect's purported residence for the particular firearm, "the affidavit does not set forth any evidence indicating that [the suspect] owned or used other firearms, that such firearms were contraband or evidence of a crime, or that such firearms were likely to be present." *Id*. The court thus held that the warrant was facially overbroad under *Spilotro*. *Id*. at 1024, 1026-28.

Here, the warrant allowed officers to search documents to determine the identity of "patrons who used the computers at the Long Haul Infoshop." Yet, the vast majority of visitors who used the computers at the Infoshop were legitimate users who did not send the emails under investigation and used the computers at other times or on entirely different days; accordingly, there was no probable cause to search for the names of any other patrons. The warrant failed to set out any standards that would allow the raid team to "differentiate items subject to seizure from those which are not." *Spilotro,* 800 F.2d at 963. Defendant Kasiske could easily have asked to search for information about who might have used the computers on the days and at the times that the emails were sent, but instead he asked for authorization to learn the names of everyone who used the computers without limitation. Zimm. Decl. Ex. 1. Kasiske's warrant thus fails all three of the *Spilotro* questions and is in fact far broader than the one found patently overbroad in *Millender*. Just

as probable cause to search for one gun could not justify the broad warrant in that case, "probable cause to search for documents pertaining to certain aspects of an operation cannot justify the seizure of all documents in an office." *Millender*, 620 F.3d at 1025 (citing *United States v. Stubbs*, 873 F.2d 210, 211 (9th Cir. 1989)); *see id*. at 1026-27 (where government knows what it needs, warrant authorizing search of "broader class of records" is invalid). And the warrant in this case falls squarely within the Ninth Circuit's holding in *United States v. SDI Future Health*, 568 F.3d 684 (9th Cir. 2009) where the court invalidated as overbroad a warrant authorizing a company's "rolodexes, address books, and calendars" on the grounds that "this category practically begs the search team to find and to seize the contact information of every person who had ever dealt with" the company when the warrant could have limited the search to encompass only categories "likely to turn up conspirators." *SDI Future Health*, 568 F.3d at 705.

Defendants' overreach is of particular concern here because the Long Haul premises is a place that activists come to use computers for their *political* activities. As this Court noted when ruling on the federal Defendants' motion to dismiss Plaintiffs' First Amendment claims, "[t]o the extent Plaintiffs also contend that Defendants' execution of the search warrant violated their First Amendment rights by obtaining information on their members' identity, the Court finds that such claims are better addressed through Plaintiffs' Fourth Amendment claims." Court Order, Docket No. 69 at 11. Searching Long Haul was an opportunity to investigate whether the organization had ties to individuals opposed to animal research specifically and to the animal rights movement more generally. Searching for this broader information went well beyond the scope of probable cause to look for the sender of the emails. This fishing expedition was improper and unlawful.

2. The Warrant Authorized the Seizure of All Storage Media, Regardless of Whether Computer Logs Were Likely to Be Stored There.

The warrant was also improper in that it authorized the seizure of "[a]ll electronic data processing and storage devices, computers and computer systems, including but not limited to central processing units, external hard drives, CDs, DVDs, diskettes, memory cards, PDAs, and USB flash drives." Zimm. Decl. Ex. 1. For this reason, too, the warrant violated *Spilotro* and resulted in the seizure of every electronic-storage device that the police found at Long Haul.

Kasiske's Statement of Probable Cause stated that the "suspect who sent the threatening email messages used" or could have used the public access computers for other purposes, therefore a search of those computers "could reveal information the suspect stored on" those machines. Zimm. Decl. Ex. 3. But the warrant authorized a much broader seizure of every conceivable type of computer or electronic storage device in the building. Zimm. Decl. Ex. 1. The Statement of Probable Cause did not explain why evidence identifying the email sender could have been contained on CDs, DVDs, PDAs, smartphones, or any devices other than the computers themselves. Zimm. Decl. Ex. 3. The warrant therefore authorized searches and seizures of entire categories of items for which there was no probable cause. This in itself renders the warrant unconstitutionally overbroad.

Nor did some other part of the warrant give the raid team objective standards to distinguish the computers for which Kasiske indicated that he needed access – the public-access computers – from other computers that could not have held evidence of who sent the emails. It would have been an easy matter for the warrant to limit its scope to the public-access computers, yet the warrant did not include this limitation.

3. The Warrant Authorized a Search "For Evidence" Without Limitation.

Finally, the warrant was also improper in that it purported to allow a search of all seized items "for evidence." Zimm. Decl. Ex. 1. The only elaboration in the warrant itself was the inclusion of checks next to the boxes in the "evidence type" section of the warrant indicating that the warrant applies to "property or things used as a means of committing a felony" or that "tend[] to show a felony has been committed, or tend[] to show that a particular person has committed a felony." *Id.* The warrant does not even mention any penal code section, or that the crime under investigation involved the transmission of harassing emails. A search "for evidence" does not come close to describing the things to be searched or seized with any kind of particularity that could guide an officer's conduct.

The Ninth Circuit has rejected far more specific descriptions of what evidence officers may seek than that set forth in the warrant here. *See United States v. Washington*, 797 F.2d 1461, 1472 (9th Cir. 1986) (generic descriptors of business records are insufficient where the whole business was not permeated by criminal activity); *United States v. Cardwell*, 680 F.2d 75, 77 (9th Cir. 1982) ("The

only limitation on the search and seizure of appellants' business papers was the requirement that they be the instrumentality or evidence of violation of the general tax evasion statute, 26 U.S.C. § 7201. That is not enough."); *Spilotro*, 800 F.2d at 965-66.

The officers' own conduct is additional proof that the warrant was insufficiently particular. For example, Shaffer and Zuniga looked at photographs of protestors in Seattle. Zimm. Decl. Ex. 7 (*Shaffer*) 55:20-56:5. Shaffer, and probably other officers, looked through EBPS's mail and left it in a jumbled pile on the floor, *id.* at 64:21-65:1, and Kasiske asked the lab to search seized computers for information about people who were suspects in other investigations he was conducting and the lab conducted this search without objection, Zimm. Decl. Ex. 25; Zimm. Decl. Ex. 21 (*Beeson*) 37:22-41:16.

As to the third *Spilotro* factor, Kasiske could have asked to search the public-access computers and logs for information from the June 2008 dates when threatening felony emails were sent, specified a search for evidence of who sent the specific emails referenced in the Statement of Probable Cause, and asked the forensic lab to search only for evidence that might help identify the person who had sent the harassing emails, rather than information about suspects in other cases, on any and all dates. However, he did not.

B. The Statement of Probable Cause Cannot Cure the Warrant's Facial Overbreadth.

1. The Statement of Probable Cause Was Not Present at Long Haul During the Search.

The search warrant itself, not supporting documents, must satisfy the Fourth Amendment's particularity requirement. *Groh v. Ramirez*, 540, U.S. 551, 557 (2004). "More specific standards may be contained in an affidavit, rather than the warrant itself, only if: '(1) the warrant expressly incorporate[s] the affidavit by reference and (2) the affidavit either is attached physically to the warrant or at least accompanies the warrant while agents execute the search.'" *Millender*, 620 F.3d at 1026 (citing *United States v. Kow*, 58 F.3d 423, 239 n.3 (9th Cir. 1995)). But where there is no evidence "that the affidavit was physically attached to the warrant or accompanied the warrant on the search… [the Court] cannot consider its effect." *Id*. Here, there is no evidence that the statement of probable cause was either attached or present at the search. Defendants Kasiske, Alberts and Zuniga

testified that they did not know or remember whether the document was present at the search, and no officer said that it was. Zimm. Decl. Ex. 5 (*Kasiske*) 72:13-17, 76:7-11; Zimm. Decl. Ex. 11 (*Alberts*) 135:9-13, 71:6-12.

More importantly, even if the "Court could consider the affidavit, it still would not cure the warrant's deficiencies" because the officers did not "rel[y] on the information in the affidavit to limit the warrant's overbreadth." *Millender*, 620 F.3d at 1026. The officers here (as discussed below) searched and seized far beyond the limits provided by the Statement of Probable Cause had they relied on it to narrow the scope of the warrant. Since Defendants did not limit the scope of their search to actions reasonably calculated to identify the sender of the March or June emails they cannot claim that the affidavit cured the warrant's overbreadth.

2. The Raid Team's Conduct During the Search Itself Was Unreasonably Intrusive.

Any search conducted pursuant to an overbroad warrant violates the Fourth Amendment. But the search here further violated the Fourth Amendment because the officers' conduct was unreasonable as the raid team Defendants searched for items unrelated to the threatening emails.

Defendants should not have searched the private offices and seized the computers and other digital media they found there. Kasiske informed the judge issuing the warrant only that there were public access computers at Long Haul that may have been used to send the threatening emails. Zimm. Decl. Ex. 3. Upon entering the premises, officers were quickly were able to see the public access computers in the back loft. Zimm. Decl. Ex. 6 (*Kasiske*) 102:17-103:12. It was also obvious to a reasonable officer that there were private offices belonging to EBPS and two other entities (the doors were adjacent, all locked and there were signs indicating the name of the tenant on the door). Zimm. Decl. Ex. 4 (*Palmer 1*) 24:14-20 (locked, adjacent offices); Palmer Decl. ¶ 10. Officers saw the East Bay Prisoner Support sign and therefore knew or should have known that the EBPS's office was separate from Long Haul since the inventory of property seized reports that certain devices were taken from the "downstairs office-East Bay Prisoners Support." Zimm. Decl. Ex. 2; *see also* Zimm. Decl. Ex. 11 (*Lyons*) 53:24-54:8, 55:7-11 (sign and lock indicated that EBPS office was not public and distinct from Long Haul). It was also obvious that the locked Slingshot office with a Slingshot

banner overhead was for the publication and not for members of the public to come in and use the computers there. Zimm. Decl. Ex. 4 (*Palmer 1*) 24:12-20, 63:20-25. Every issue of Slingshot since April of 1994 says that it is published from that Shattuck Avenue address, and there were multiple copies of Slingshot visible throughout the premises and in the office. *See*, *e.g.*, Palmer Decl. ¶ 26; *id*. Ex. 16 (photograph of Slingshot news rack on the Long Haul premises).

When officers are executing a search warrant and discover (or reasonably should have discovered) that a building has multiple units or tenants they cannot search those areas without further authorization. *Mena v. City of Simi Valley*, 226 F.3d 1031, 1038 (9th Cir. 2000) (search unreasonable when officers observed that the rooms within the unit were padlocked from outside, and once entry was forced to rooms, that the rooms were set up as studios).

Defendants may argue that because the threatening emails traced back to Long Haul's IP address, they were entitled to seize any computer on the premises, without regard for who owned or used it, or where it was stored. However, the private computers were unmentioned in the warrant application, and they only could be seized if they were likely to contain evidence of who sent the threatening emails. *Payton*, 573 F.3d at 864. No such likelihood existed. Defendants had no information, for example, that the Slingshot and EBPS computers shared the offending IP address with each other or with the public access computers. *See* Zimm. Decl. Ex. 6 (*Kasiske*) 137:1-11 (no specific knowledge about IP addresses at Long Haul). As in *Payton*, officers had no indicia that relevant information would be found on the computers.

Moreover, the decision was not one for the officers to make. At the very least, what raid team Defendants should have done, once they realized that there were private offices containing unexpected computers on site, was to go back to the judge to demonstrate (1) probable cause to believe that these machines were also assigned the IP Protocol address used by the email sender at the time of transmission; (2) why they needed to seize these computers; and (3) how they would search these machines to segregate private data from evidence of the email crime to the extent possible. This is what officers did in *United States v. Giberson,* 527 F.3d 882, 884-86 (9th Cir. 2008) (officers searching pursuant to warrant for evidence that resident was creating fake identification documents found such documents next to computer and printer, secured the computer, and sought second

warrant which authorized the seizure and subsequent search of that computer for fake identification evidence). Since computer searches inevitably involve intermingled data and require extra care, *Hill*, 459 F.3d at 973, this kind of judicial supervision is particularly important. *United States v. Tamura*, 694 F.2d 591, 596 (9th Cir. 1982), requires officers seizing intermingled data to, at the very least, "seal[] and hold[] the documents pending approval by a magistrate of a further search." *See also United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1170-71 (9th Cir. 2010) (holding that investigators violated *Tamura* when they failed to segregate drug test results for larger group of athletes from those few tests authorized for seizure in the warrant).

The search of the Slingshot and EBPS offices also went too far. Just as a warrant to search a house for firearms does not authorize the police to look in spaces too small to hold a gun, the warrant here could authorize the raid team to search for evidence in places where it could not possibly be found. Yet the officers examined photographs of anti-war demonstrators in Seattle that could not possibly have been relevant to the alleged cause for the search. Zimm. Decl. Ex. 8 (*Shaffer*) 55:23-56:11 (Zuniga showed Shaffer photograph from Seattle war demonstration because she came from Seattle office). Zimm. Decl. Ex. 9 (Shaffer's Resp. to Pl.'s First Set of Interrogs. # 8) (Shaffer examined "5-6 photos of scenes of downtown Seattle, including one she recalls as a photo of an old police vehicle"). Officers also went through EBPS mail. Zimm. Decl. Ex. 8 (*Shaffer*) 64:21-65:1; Zimm. Decl. Ex. 9 (Shaffer's Resp. to Pl.'s First Set of Interrogs. # 8) (Shaffer "looked at two envelopes that she concluded were either addressed to or from prisoners"); Zimm. Decl. Ex. 11 (*Lyons*) 87:15-23 (all of EBPS's mail, including approximately 50 to 100 letters, was strewn about, taken off shelves, and out of envelopes). And, though Long Haul kept no logs of visitors to the public access computer room, (Palmer Decl. ¶ 9) Defendants Alberts and Shaffer paged through sensitive library lending logs and lists of volunteers. Miller Decl. ¶ 5; Zimm. Decl. Ex. 10 (*Miller*) 74:18-22; Zimm. Decl. Ex. 12 (*Alberts*) 100:6-17; Zimm. Decl. Ex. 8 (*Shaffer*) 51:22-52:4; Zimm. Decl. Ex. 9 (Shaffer's Resp. to Pl.'s First Set of Interrogs. # 8).

II. DEFENDANTS VIOLATED THE PRIVACY PROTECTION ACT

In addition to violating the Fourth Amendment, the raid team Defendants violated the Privacy Protection Act ("PPA") by seizing documentary and work product materials in violation of

the statute. The PPA was adopted in response to the Supreme Court's ruling in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), to protect the electronic and paper files of both traditional media and also of organizations like Long Haul and EBPS that communicate to the general public through newspapers or other public communications. *See* S. Rep. 96-874, at 4 (1980), *reprinted* 1980 U.S.C.C.A.N. 3950, 3951 ("The Committee believes that the search warrant procedure in itself does not sufficiently protect the press and other innocent third parties and that legislation is called for").

A. Defendants Seized Work Product Materials in Violation of the PPA.

It is "unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication" unless the government shows that one of the two listed exceptions applies. 42 U.S.C. §§ 2000aa(a). Work product materials are "materials, other than contraband or the fruits" or instrumentalities of a crime, that were (1) "prepared, produced, authored, or created, whether by the person in possession of the materials or by any other person", "in anticipation of communicating such materials to the public"; "(2) are possessed for the purposes of communicating such materials to the public; and (3) include mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored, or created such material." 42 U.S.C. § 2000aa-7(b).

Defendants seized hundreds of electronic documents from the Slingshot office that are protected work product materials: the two Slingshot computers contained hundreds of articles and drafts of articles that had been written and submitted for publication. Palmer Decl. ¶ 21; *id.* Exs. 12-15 (sample of documents contained on the seized Slingshot computers). Defendants seized the computers containing these documents, copied the documents off the computer hard drives, and still retain that data. Zimm. Decl. Ex. 30; Zimm. Decl. Ex. 31 (Alberts' Resp. to Pl.'s Req. for Admis. # 21); Zimm. Decl. Ex. 13 (Celaya's Resp. to Pl.'s Req for Admis. # 20, 21).

Defendants are liable because a reasonable officer in the same position would have known that the Slingshot computers contained documents created for the purpose of disseminating information to the public. Plaintiff Long Haul has published the quarterly newspaper Slingshot

continuously since 1993 out of its Shattuck Street address. The newspaper is distributed on and around the University of California, Berkeley campus, where the UC Defendants work. In February of 2008, Defendant Zuniga forwarded to his supervisor, Defendant Alberts, an email linking to an online Slingshot article. Zimm. Decl. Ex. 26. Zuniga wrote that, on its webpage, Slingshot "claim[s] an affiliation with The Long Haul on 3124 Shattuck Ave here in Berkeley." *Id.* The original author of the forwarded email opined that Slingshot was authored by the animal activists that UC investigators were monitoring, or by someone close to them. The author also forwarded the Slingshot link to Defendant Shaffer's employer, the FBI. *Id*. (The Slingshot website, like the physical paper, indicates that it is located at the same address as Long Haul. Palmer Decl. ¶ 12.) At the time, the Long Haul website also contained a link to Slingshot's webpage under the heading "Individual Collectives at the Long Haul." Palmer Decl. ¶ 12; *id*. Ex. 1. During his preparation of the search warrant affidavit, Defendant Kasiske reviewed the Long Haul website. Officer MacAdam and Agent Shaffer also knew that Slingshot was a publication at the time of the raid. Zimm. Decl. Ex. 22 (MacAdam Resp. to Pl.'s First Set of Interrogs. # 13); Zimm. Decl. Ex. 9 (Shaffer Resp. to Pl.'s First Set of Interrogs. # 10).

In addition to knowing that Slingshot and Long Haul were affiliated, that Slingshot was located at the Long Haul address, and that Slingshot was a publication, the raid team members encountered an upstairs locked office with a large banner sign over the that said "Slingshot." Palmer Decl. ¶ 17; *id*. Ex. 8. A Slingshot news rack stood in the foyer just inside Long Haul's front door. Palmer Decl. ¶ 26; *id*. Ex. 16. At least Defendants Shaffer and Alberts saw Slingshot newspapers in the Slingshot office. Zimm. Decl. Ex. 23 (Alberts' Resp. to Pl.'s First Set of Interrogs. # 8); Zimm. Decl. Ex. 9 (Shaffer's Resp. to Pl.'s First Set of Interrogs. # 10). Thus, at the time they seized computers from inside the Slingshot office, a reasonable officer would have known that the documents on those computers were possessed with the purpose of disseminating information to the public.

Ignorance is no defense. The standard under the PPA is whether the officers *reasonably believed* the seized materials to belong to someone in the business of disseminating information to the public. All the facts available to the officers strongly lead to the reasonable conclusion that the

Slingshot computers contained PPA protected materials. If it was somehow unclear to any officer that the upstairs office belonged to Slingshot, whether Slingshot property was stored inside Long Haul, or whether the Slingshot computers contained protected materials, the officer was obligated to stop the search and do further investigation. *Motley v. Parks*, 432 F.3d 1072, 1081 (9th Cir. 2005) (while conducting investigations, all officers have an ongoing duty to make appropriate inquiries regarding the facts received or to further investigate if insufficient details are relayed). Lead investigator Kasiske was at the very least uncertain whether he had seized protected materials. When he submitted his request for the lab to perform forensic analysis on some of the Long Haul hard drives, Kasiske was asked to indicate whether the materials to be analyzed were protected by the PPA or otherwise privileged. Defendant Kasiske responded "Not Sure". Zimm. Decl. Ex. 32. Defendants' failure to investigate whether they had seized and retained privileged materials is a violation of their legal duties when performing searches and seizures.

Defendants also seized work product materials from EBPS. Lyons Decl. ¶ 3. At the time of the raid, Long Haul's website which Kasiske reviewed stated that EBPS had a "prison-related book/zine/video library" and that it hosted a regular event where people would "read and reply to prisoner mail" and "correspond with Political Prisoners." Palmer Decl. ¶ 11; *id.* Ex. 1. Upon entering Long Haul, officers found the locked and labeled EBPS door in a hallway of other locked offices with the names of different organizations on the doors. Officers could have searched for EBPS on the Internet and would have found the group's Myspace page, which indicated that EBPS possessed "information about political prisoners, prison conditions, grand jury resistance, security culture, campaigns, event information, and resources for prisoners" as well as a "prison-related zine, book, and video library." Lyons Decl. ¶ 4.

The raid team nevertheless entered the private office, went through a stack of mail in the EBPS office and seized the EBPS computers, which contained drafts of articles as well as names, addresses, and email addresses of infoshops, distributors, publishers and other groups to which EBPS distributed prisoner-related literature and from which EBPS received literature. Lyons Decl. ¶ 3; Zimm. Decl. Ex. 10 (*Lyons*) 91:8-15; Zimm. Decl. Ex. 17 (*Harris*) 73:24-74:3. A reasonable officer knowing that EBPS hosted a regular event at Long Haul to distribute information to prisoners, and

that EBPS had a locked office at Long Haul, would have known that the EBPS computers contained materials possessed with the intent to distribute information to the public. At the very least, a reasonable officer familiar with the Long Haul website and its announcement about the regular EBPS letter writing event and library, upon encountering the locked EBPS office with the East Bay Prisoner Support sign, has a duty to investigate whether the office is rented by another tenant and off limits and whether the office contains the library and other materials the group advertises as being possessed for distribution to the public. *Maryland v. Garrison*, 480 U.S. 79, 88 (1987) (the validity of the search of a private apartment pursuant to a warrant authorizing the search of the entire third floor depends on whether the officers' failure to realize the overbreadth of the warrant was objectively understandable and reasonable); *Motley*, 432 F.3d 1072, 1081. Raid team officers failed to make any such investigation or to restrain themselves from searching and seizing EBPS's documents, despite acknowledging that this particular downstairs office was labeled as belonging to EBPS. Zimm. Decl. Ex. 2.

B. Defendants Seized Documentary Materials in Violation of the PPA.

The PPA defines "documentary materials" to include essentially any type of recorded information other than the fruits or instrumentalities of a crime, specifically including photographs and printed and electronic documents. 42 U.S.C. § 2000aa-7(a). It is "unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, search for or seize documentary materials, other than work product materials, possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication," unless one of the four listed exceptions apply. 42 U.S.C. § 2000aa(b). This provision differs from the section in that it covers many more types of material and applies whenever they are possessed by a person in connection with publication, regardless of whether the police know this fact.[4] Also, it provides a lesser *degree* of protection because there are more exceptions that the police can invoke.

[4] This standard does not eliminate a knowledge requirement because officers who do not know they are searching protected materials may be able to invoke the good-faith defense under 42 U.S.C. § 2000aa-6(b). For the reasons stated, Defendants have no basis to assert that defense here.

Defendants searched and seized documentary materials. As described above, Defendant raid team members searched through photographs in the Slingshot office that had been collected for publication in the newspaper, as well as other files that were used in publishing the newspaper. The seized Slingshot computers also contained a broad array of documentary materials that Slingshot had collected as part of its operation. Zimm. Decl. Ex. 10 (*Miller*) 48:14-49:15. Defendants Zuniga and MacAdam also entered the locked EBPS office where Agent Shaffer searched the mail and left correspondence in disarray. Zimm. Decl. Ex. 8 (*Shaffer*) 67:19-23; Zimm. Decl. Ex. 9 (Shaffer Resp. to Pl.'s First Set of Interrogs. # 8). The officers also seized computer hardware and compact disks from the EBPS office equipment that contained material that had been collected in order to distribute it to the public. Zimm. Decl. Ex. 6 (*Kasiske*) 110:5-9; Zimm. Decl. Ex. 18 (*Harris*) 73:24-74:3; Lyons Decl. ¶ 2.

III. Each Raid Team Defendant is Individually Liable as an Integral Participant in the Unlawful Search.

State and federal law enforcement officers who violate the Fourth Amendment are liable to the injured parties under 42 U.S.C. § 1983 and *Bivens*, 403 U.S. at 392, respectively. "It is incumbent on the officer executing a search warrant to ensure the search is lawfully authorized and lawfully conducted." *Groh*, 540 U.S. at 563. Thus, every officer who enters and conducts a search under the authority of an unconstitutionally overbroad warrant is liable in damages, as are the officers who obtained that warrant. *See Millender*, 620 F.2d at 1024; *id*. at 1034-35 (denying qualified immunity for "obtaining and executing the warrants"). Additionally, officers have an independent responsibility to investigate when the information they are given in an investigation is inadequate. *Motley*, 432 F.3d 1072, 1081.

Moreover, every officer who is an "integral participant" in a search is liable for Fourth Amendment violations committed by other officers during the search, regardless of whether the individual "officer's actions themselves rise to the level of a constitutional violation." *Boyd v. Benton County*, 374 F.3d 773, 780 (9th Cir. 2004) (citing *Melear v. Spears*, 862 F.2d 1177 (5th Cir. 1989)). All raid team Defendants were far more than "mere bystanders." *Chuman v. Wright*, 76 F.3d 292, 294 (9th Cir. 1996). Each officer was an active member of the Animal Rights Working Group,

participated in the planning meeting, and provided armed guard at the raid. *See Melear*, 862 F.2d 1177. Each officer also either searched paper files, photographs, mail or other logs, seized computers and placed them in police cars, or some combination thereof. Supervisors are further liable for acquiescing in the wrongful acts of their subordinates. *Blankenhorn v. City of Orange*, 485 F.3d 463, 485 (9th Cir. 2007).

Specifically, Defendant Kasiske led this investigation, prepared the search warrant, conducted the pre-search briefing, and searched all the rooms in the building. Zimm. Decl. Ex. 6 (*Kasiske*) 97:9-101:18. He also submitted the requests for forensic analysis to the forensic lab and defined the search terms. Zimm. Decl. Ex. 6 (*Kasiske*) 132:5-11.

Defendant Alberts was extensively involved in the investigation that led up to the search, including monitoring activities at the Long Haul, consulting with the other investigators in email exchanges regarding the investigation and search warrant, and supervising Kasiske. Alberts also searched the front cabinet as well as various rooms at Long Haul. Zimm. Decl. Ex. 23 (Alberts Resp. to Pl.'s First Set of Interrogs. # 9); Zimm. Decl. Ex. 12 (*Alberts*) 12:5-8, 63:22-65:13, 98:23-99:11; Zimm. Decl. Exs. 28, 29.

Defendant MacAdam provided security for the search, entered the building and cut, jimmied or unscrewed locks on all secured areas at the premises. Zimm. Decl. Ex. 15 (*MacAdam*) 50:6-9, 67:8-10. Defendant Zuniga searched the Slingshot office, including the Seattle photos, and carried computers to the waiting cars. Zimm. Decl. Ex. 7 (*Zuniga*) 48:21-23; Zimm. Decl. Ex. 24 (Zuniga's Resp. to First Set of Pl.'s Interrogs. # 8).

Defendants Shaffer and Hart were also integral participants in the raid. Both were part of the Animal Rights Working Group. Defendant Alberts discussed the search warrant with Shaffer early in the investigation. Zimm. Decl. Ex. 8 (*Shaffer*) 14:23-15:9; Zimm. Decl. Ex. 12 (*Alberts*) 36:9-23. Shaffer attended the pre-raid briefing, participated in the search, searched the photo file in the Slingshot office (even though it was unrelated to the investigation at hand), looked through prisoner mail in the EBPS office, and helped seize and remove computer hardware from the premises. Zimm. Decl. Ex. 8 (*Shaffer*) 7:9-18, 26:23-27:1, 55:24-56:21, 64:22-65:15, 66:23-67:1.

Defendant Hart was assigned to assist with security and with searching the Long Haul premises. Zimm. Decl. Ex. 6 (*Kasiske*) 66:16-22. He attended the pre-raid planning meeting. *Id*. at 64:8-9. During the raid, Hart provided armed guard as the other officers entered and searched the premises and seized materials there. Zimm. Decl. Ex. 12 (*Alberts*) 132:1-4. He also went inside and seized computers. Zimm. Decl. Ex. 12 (*Alberts*) 131:23-132:13. This is exactly the type of involvement that makes an officer an "integral participant" under *Boyd* and *Millender*. *See also James v. Sadler,* 909 F.2d 834, 837 (5th Cir. 1990) (armed officers who did not pat down the plaintiff and stayed on the lawn were integral to the search and liable); *Melear*, 862 F.2d, 1177 (officer who does not enter an apartment, but stands at the door, armed with his gun, while other officers conduct the search, can be a "full, active participant" in the search), *Cf. Jones v. Williams*, 297 F.3d 930 (9th Cir. 2002) (where plaintiff knows only that defendant officer was armed but nothing else, officer is not liable as a integral participant).

All raid team officers were integral participants in the unlawful search and are thus liable for all the violations. Finally, the United States is liable for its employee's violations of the PPA. 42 U.S.C. § 2000aa-6(a). Hart and Shaffer individually violated the PPA in that Shaffer searched documentary materials and Hart carried computers containing documentary and work product materials to waiting police cars.

IV. CONCLUSION

For the above reasons, Plaintiffs respectfully asks this Court to grant its motion for summary judgment that Defendants Alberts, Kasiske, MacAdam, Zuniga, Bauer, Hart and Shaffer are individually liable for damages in an amount to be determined for violating the Fourth Amendment and Privacy Protection Act and are liable in their official capacities for equitable and declaratory relief under the Fourth Amendment and 28 U.S.C. §§ 2201, 2202, that the United States is liable for damages in an amount to be determined for violating the Privacy Protection Act, and that Defendant Celaya is liable in his official capacity for equitable and declaratory relief under the Fourth Amendment and 28 U.S.C. §§ 2201, 2202.

DATED: January 31, 2011

By */s/ Jennifer Stisa Granick*
JENNIFER STISA GRANICK

c/o ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x127
Facsimile: (415) 436-9993

COUNSEL FOR PLAINTIFFS