UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

PASCAL ABIDOR, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, NATIONAL PRESS PHOTOGRAPHERS ASSOCIATION, Plaintiffs, v. JANET NAPOLITANO, in her official capacity as Secretary of the U.S. Department of Homeland Security; ALAN BERSIN, in his official capacity as Commissioner, U.S. Customs and Border Protection; JOHN T. MORTON, in his official capacity as Assistant Secretary of Homeland Security for U.S. Immigration and Customs Enforcement, Defendants.	Case No. 1:10-cv-04059 (Korman, J.) (Azrack, M.J.)

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

CATHERINE CRUMP
HINA SHAMSI
BENJAMIN T. SIRACUSA HILLMAN
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2583
ccrump@aclu.org

(additional counsel on following page)

MICHAEL PRICE
National Association of Criminal Defense Lawyers
1660 L Street NW, 12th Floor
Washington, DC 20036
(202) 872-8600

CHRISTOPHER DUNN
MELISSA GOODMAN
ARTHUR EISENBERG
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
(212) 607-3300

March 9, 2011

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

PRELIMINARY STATEMENT

Plaintiffs bring this action to challenge Department of Homeland Security (DHS) policies that authorize the suspicionless search and detention of Americans' laptops, cell phones, and other electronic devices at the international border. With each passing day, Americans conduct more of their lives electronically, storing their most intimate details on their personal electronic devices, which have become extensions of people's minds and receptacles for their thoughts and memories. This case challenges the government's claimed authority to search Americans' most private details without any reasonable suspicion of wrongdoing. The DHS policies purport to authorize the government to scrutinize without any suspicion international travelers' diary entries, financial records, family photographs, medical records, personal correspondence, information subject to the attorney-client and other legal privileges, and confidential interviews with clients and sources. Moreover, the policies state that the government can detain electronic devices that contain this information, or copies of this information, and continue to search them after travelers have left the border, for as long as the government likes, also without any suspicion. Plaintiffs oppose defendants' motion to dismiss this case.

Plaintiffs are a U.S. citizen and two professional organizations. Compl. ¶ 2. Pascal Abidor is a U.S. citizen who studies at McGill University in Montreal. A DHS employee searched Mr. Abidor's laptop for no reason other than that he was pursuing a Ph.D. in Islamic Studies and had traveled to the Middle East. *Id.* ¶¶ 27-31. He was removed from a train in handcuffs and held and questioned for three hours while officials searched his laptop. Although Mr. Abidor was ultimately permitted to enter the country, DHS did not return all of his electronic devices to him, including his laptop, for 11 days,

during which time DHS viewed Mr. Abidor's photographs and read his emails, tax returns, and notes. *Id.* ¶¶ 34, 36, 41, 50, 51. The National Association of Criminal Defense Lawyers and National Press Photographers Association have over 40,000 members between them and have members whose electronic devices have been searched at the border. *Id.* ¶¶ 66, 85, 100, 120. Lawyers and journalists have a professional, ethical, and in the case of lawyers, often a legal obligation to hold their clients' and sources' information in confidence. *Id.* ¶¶ 78-79, 111-114, 117. The policies pose a serious impediment to the organizations' members' ability to do their jobs. *Id.* ¶¶ 77-83, 110-118.

Plaintiffs filed this lawsuit because the DHS policies violate the Fourth and First Amendments. DHS's claimed authority to engage in unlimited searches of Americans' private expressive materials, without any reasonable suspicion, poses a grave threat to the values of privacy and free speech. The Fourth Amendment's prohibition on unreasonable searches and seizures prohibits the boundless and standardless searches authorized by the DHS policies. Likewise, a purely suspicionless search policy violates the robust protections for personal, expressive materials that the First Amendment provides.

BACKGROUND

When reviewing a motion to dismiss under Fed. R. Civ. P. 12(b)(1) or 12(b)(6), "the court must accept all factual allegations in the complaint as true and draw inferences from those allegations in the light most favorable to the plaintiff." [1] *Jaghory v. N.Y. State Dep't of Educ.*, 131 F.3d 326, 329 (2d Cir. 1997). Plaintiffs' Complaint alleges:

[1] Defendants attach four exhibits to their motion. Even if it may sometimes be appropriate to consider evidence outside the pleadings in determining whether to grant a motion to dismiss under Rule 12(b)(1), *see Alliance for Envtl. Renewal, Inc. v. Pyramid*

I. The Border Search Policies

In August 2009, two DHS components issued similar policies regarding the search and detention of electronic devices at the border. U.S. Customs and Border Protection (CBP), "Border Search of Electronic Devices Containing Information," Directive No. 3340-049 (Aug. 20, 2009) (Defs.' Br. Ex. B) ("CBP Policy"); U.S. Immigration and Customs Enforcement (ICE), "Border Searches of Electronic Devices," Directive No. 7-6.1 (Aug. 18, 2009) (Defs.' Br. Ex. A) ("ICE Policy").

Both policies permit border officials to read and analyze information on international travelers' electronic devices without reasonable suspicion. CBP Policy § 5.1.2; ICE Policy § 6.1. Although the CBP policy states that searches of electronic devices should be conducted in the presence of a supervisor, the requirement is waived

---

Crossgates Co., 436 F.3d 82, 87-88 & n.8 (2d Cir. 2006), the only exhibit upon which defendants rely to support their Rule 12(b)(1) motion is the Riley Declaration, which plaintiffs discuss in greater detail in Part I.A, *infra*. Matters outside of the pleadings may not be considered on a motion to dismiss under Rule 12(b)(6) "without converting the motion into a motion for summary judgment." *Courtenay Commc'ns Corp. v. Hall*, 334 F.3d 210, 213 (2d Cir. 2003). Defendants, however, are not seeking to convert their Rule 12(b)(6) motion into one for summary judgment and doing so would be inappropriate in any event because there has been no opportunity for discovery.

Besides the Riley Declaration, defendants attached three additional exhibits to their memorandum of law: the CBP and ICE policies and a press release. Defs.' Br. Exs. A-C. As a matter outside the pleadings and because it is inadmissible hearsay, the press release should be stricken. As for the policies, plaintiffs described them in their Complaint, and do not dispute that defendants' attachments are accurate copies of the policies. For the Court's convenience, plaintiffs, like defendants, cite directly to the policies. However, plaintiffs do not concede the correctness of assertions contained within the policies, such as what electronic device searches allegedly accomplish, and defendants may not assert the truth of such assertions in support of their Rule 12(b)(6) motion.

Plaintiffs attach a declaration to their response. Plaintiffs have no intention of converting defendants' Rule 12(b)(6) motion to one for summary judgment; rather, they attach the declaration for the purpose of responding to defendants' Rule 12(b)(1) argument that Mr. Abidor lacks standing because he faces no threat of immediate harm. *See Rosenbaum v. City & County of San Francisco,* 8 F. App'x 687, 690-91 (9th Cir. 2001); *Rosenbaum v. City & County of San Francisco*, 484 F.3d 1142, 1149, 1151-52 (9th Cir. 2007).

where "operational considerations" interfere or where supervision is "not practicable." CBP Policy § 5.1.3. The ICE policy contains no provision for supervision. Although both policies state that searches should be conducted in the traveler's presence, the requirement is waived where "operational considerations" make a traveler's presence "inappropriate." CBP Policy § 5.1.4; *see also* ICE Policy § 8.1(2). Even where a traveler is permitted to be present, that does "not necessarily mean that the individual will be permitted to witness the search itself." CBP Policy § 5.1.4; ICE Policy § 8.1(2).

Both policies permit border officials to read and analyze—without reasonable suspicion—even legal or privileged information, information carried by journalists, medical information, confidential business information, and other sensitive information. The ICE policy states unequivocally that "a claim of privilege or personal information does not prevent the search of a traveler's information at the border." ICE Policy § 8.6(1). CBP policy states that "legal materials" "may be subject" to the requirement that an agent "seek advice" from counsel. CBP Policy § 5.2.1. It does not require agents to seek such advice. It does not indicate that there are circumstances in which counsel will recommend having reasonable suspicion before commencing a search. As for other sensitive information, the policies provide only that they shall be handled in accordance with "any applicable federal law and . . . policy." CBP Policy § 5.2.2; *see also* ICE Policy § 8.6(2)(a)-(c). The policies do not specify any law or policy that might require reasonable suspicion, and the policies themselves contain no such requirement.

Both policies permit border officials, without any suspicion of wrongdoing, to detain a traveler's electronic devices, or the information they contain, for further reading, scrutiny, and copying even after the traveler has left the border, and for a potentially

unlimited time. CBP Policy § 5.3.1; ICE Policy § 8.1(4). The policies specify that travelers' devices or the information they contain may be removed from the port and sent elsewhere. CBP Policy § 5.3.1; ICE Policy § 8.1(4). The policies do not explain, or limit, where travelers' devices or information may be sent. The policies do not place time limits on how long ICE and CBP may detain travelers' devices or the information they contain or continue to read and analyze the information. While the policies provide for intermittent supervisory approvals as detentions continue, they also provide for limitless extensions. CBP Policy § 5.3.1.1; ICP Policy § 8.3. At no point during the potentially limitless detention and search period is there a requirement of reasonable suspicion. Both policies also permit border officials to share devices or the information they contain with other agencies to obtain "technical assistance" without reasonable suspicion, or "subject matter assistance" where there is reasonable suspicion. CBP Policy § 5.3.2.2 - .3; ICE Policy § 8.4(1)-(2).

Not only can CBP and ICE search and detain travelers' electronic devices without reasonable suspicion, they, other federal agencies, and state, local and foreign governments can permanently retain travelers' information. CBP and ICE may retain information relating to immigration, customs, and other enforcement matters obtained from an electronic device search, even without probable cause. CBP Policy § 5.4.1.2; ICE Policy § 8.5(1)(b). Once information is permanently retained, nothing in the policies limits the authority of CBP and ICE to share that information. CBP Policy § 5.4.1.3; ICE Policy § 8.5(1)(c). In addition, agencies that obtain information as part of a request for technical or subject matter assistance may retain that information on their own authority. CBP Policy § 5.4.2.3; ICE Policy § 8.5(2)(c).

The government's policy of engaging in suspicionless searching and detention of electronic devices and the information they contain at the international border dates back to at least July 2007. U.S. CBP, "Policy Regarding Border Search of Information" (July 16, 2008), *available at* http://1.usa.gov/96s788; U.S. CBP, "Interim Procedures For Border Search/Examination of Documents, Papers and Electronic Information" (July 5, 2007), *available at* http://bit.ly/i7NWGw, at 8.

II. Plaintiffs' Injuries

A. Pascal Abidor

Pascal Abidor is a U.S.-French dual citizen and a graduate student in Islamic Studies at McGill University in Canada. Compl. ¶ 21. On May 1, 2010 Mr. Abidor took a train home from Canada to visit his family at the end of the academic year. He was carrying his laptop, digital camera, two cell phones, and external hard drive. *Id*. ¶ 24. When the train arrived at the border, a CBP officer boarded the train and approached Mr. Abidor. *Id*. ¶¶ 25-26. In response to the officer's questions, Mr. Abidor explained that he lives in Canada because he is pursuing a graduate degree in Islamic Studies, and that in the past year he had briefly lived in Jordan and had been to Lebanon. *Id*. ¶¶ 27-28.

The officer directed Mr. Abidor to gather his belongings and led him to the café car of the train. *Id*. ¶ 29. Once they were there, she took out Mr. Abidor's laptop, turned it on, and ordered Mr. Abidor to enter his password. *Id*. ¶¶ 30-31. She then proceeded to go through his files and asked Mr. Abidor about personal pictures she found as well as pictures that Mr. Abidor had downloaded from the Internet for research purposes, including images of Hamas and Hezbollah rallies. Mr. Abidor explained that he had the rally photos because he researches the modern history of Shiites in Lebanon. *Id*. ¶ 32.

Officers then told Mr. Abidor that he would be taken off the train. A male officer directed him to put his hands against the wall. He patted Mr. Abidor down, placed him in handcuffs, and led him off the train to the port. *Id*. ¶ 34. There, Mr. Abidor was put in a detention cell without his luggage. *Id*. ¶ 35. He was questioned for about three hours, on topics including his parents, travel history and plans, Ph.D. research topic, and his perspective on the Middle East, as well as about the meaning of "symbolic materials" in his possession. *Id*. ¶ 37. He was fingerprinted and photographed. *Id*. ¶ 38.

When Mr. Abidor was released, officers told him that his laptop and external hard drive were being detained. *Id*. ¶ 42. Eleven days later, Mr. Abidor received his laptop and external hard drive via mail. *Id*. ¶ 48. By viewing the "last opened" date of his files, Mr. Abidor learned that officers had examined many of them, including personal photos, a transcript of a chat with his girlfriend, email correspondence, class notes, journal articles, his tax returns, his graduate school transcript, and his resume. *Id*. ¶¶ 50-51.

Mr. Abidor's electronic devices are likely to be searched and detained in the future pursuant to the suspicionless search policies. *Id*. ¶ 55. In fact, in December 2010, when Mr. Abidor crossed the border from Canada into New York, CBP required him to turn over his two cell phones, which were then taken out of sight. Ex. A ¶ 7. As a graduate student, Mr. Abidor will travel frequently across the border, both to visit his family and to conduct research in foreign countries, including Syria and Lebanon. *Id*. ¶¶ 55-59. Mr. Abidor has also expended time and money to minimize the injury future searches will cause, at the expense of his educational goals. *Id*. ¶ 60. He now travels with less information on his computer, self-censors what photographs he downloads, and backs up onto an external hard drive and then deletes materials he fears that border

officials may misconstrue. *Id*. ¶ 62. He now avoids taking notes for his research and gathering materials of the type that might by misconstrued by border officials and warns research subjects that he cannot guarantee them confidentiality. *Id.* ¶ 63.

B. National Association of Criminal Defense Lawyers

The National Association of Criminal Defense Lawyers (NACDL) is an organization with about 45,000 members and affiliate members that encourages the integrity, independence and expertise of criminal defense lawyers. Compl. ¶¶ 65-66. NACDL members are likely to be subjected to the suspicionless search policies in the future. Many NACDL members routinely travel abroad to collaborate with foreign colleagues and/or as part of their representation of their clients. *Id*. ¶¶ 69-70. They almost always travel with electronic devices, which are necessary to take notes, record interviews, perform legal research, draft legal documents, retrieve case files, and communicate. *Id*. ¶ 75. While traveling abroad for work purposes, they generate privileged or confidential information. *Id*. ¶ 82.

Because NACDL members have an ethical duty to safeguard attorney-client and other privileged information, *id*. ¶ 78, they must spend time and money to mitigate the harm that future searches will cause. *Id.* ¶ 81. The challenged policies purport to authorize the same federal government that is investigating or prosecuting NACDL members' clients to search this information at will. *Id*. ¶ 79. To avoid disclosing privileged information, some NACDL members refrain from taking notes or making recordings of certain meetings while abroad. *Id*. ¶ 83.

At least one NACDL member has already been subjected to a suspicionless search of her laptop. *Id*. ¶ 85. In August 2008 Lisa M. Wayne returned to the United States

from Mexico on a commercial flight and entered the country at Houston, Texas. *Id*. ¶¶ 89-90. At the airport, a CBP officer searched through Ms. Wayne's luggage and then directed her to turn on her laptop computer and enter her password. *Id*. ¶ 92. The CBP officer took Ms. Wayne's computer out of sight for more than 30 minutes. *Id.* ¶ 95.

C. National Press Photographers Association

The National Press Photographers Association (NPPA) is an organization with about 7,000 members that vigorously promotes freedom of the press. Compl. ¶¶ 99-101. NPPA members are likely to be subjected to the suspicionless search policies in the future. Many NPPA members routinely travel abroad to cover global news stories or because they specialize in travel news and photography. *Id*. ¶ 102. They invariably travel with electronic devices, including cameras, laptops and cell phones, which are necessary to capture and document images, video, and audio. *Id*. ¶¶ 104, 107.

Because NPPA members cannot avoid crossing the border with their electronic devices, they must take steps to avoid the harm an attendant search will cause. *Id*. ¶ 116. The challenged policies undermine NPPA members' ability to guarantee confidentiality to the sources they communicate with abroad. *Id*. ¶ 117. The risk that sources' identities will be revealed to border agents—and potentially shared with other parts of the U.S. government or foreign governments—will lead some sources who otherwise would have shared information or been recorded, photographed, or videotaped to decline to do so. *Id*.

Some NPPA members have already had their electronic devices searched by border officials. For example, in July 2007 Duane Kerzic returned to the United States from Canada, where he had been taking photographs for a piece on lighthouses. *Id*. ¶ 122. His laptop and camera equipment were in the saddlebag of the motorcycle he rode.

Id. ¶ 123. CBP agents referred Mr. Kerzic to secondary screening. *Id*. ¶ 124. He observed CBP agents going through his belongings. Mr. Kerzic saw the agent sit down at a desk, turn his computer on, and peruse the contents of his laptop for approximately 15 minutes. *Id*. ¶ 125. As a travel and landscape photographer, Mr. Kerzic travels frequently across the U.S. border with his electronic devices. *Id*. ¶ 127.

ARGUMENT

Defendants have moved to dismiss this case for lack of standing under Fed. R. Civ. P. 12(b)(1) and for failure to state a claim under Fed. R. Civ. P. 12(b)(6). "[T]he standard for reviewing standing at the pleading stage is lenient." *Baur v. Veneman*, 352 F.3d 625, 636-37 (2d Cir. 2003). Similarly, a case must not be dismissed pursuant to Rule 12(b)(6) so long as plaintiffs' complaint contains "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Matson v. Bd. of Educ.*, 631 F.3d 57, 63 (2d Cir. 2011) (quoting *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009)).

Defendants' argument that plaintiffs have not demonstrated an injury sufficient to confer standing lacks merit. Defs.' Br. 2. Plaintiffs have offered concrete evidence that they meet the injury requirement, for two independently sufficient reasons: (1) plaintiffs have demonstrated an actual and well-founded fear that their electronic devices will be searched and detained in the future under the policies because not only have they or their members already had their laptops searched under the policies, but they also frequently travel overseas; and (2) the current adverse impact of the policies, which require plaintiffs or their members to expend resources to mitigate the policies' harm, is a form of specific, objective, concrete injury that confers standing, *Bordell v. Gen. Elec. Co.*, 922 F.2d 1057, 1060-61 (2d Cir. 1991). Moreover, Mr. Abidor has standing for the additional reason that

he seeks expungement of data obtained from his electronic devices that he believes DHS continues to retain. *Tabbaa v. Chertoff*, 509 F.3d 89, 96 n.1 (2d Cir. 2007).

Defendants' contention that plaintiffs have failed to state a claim upon which relief can be granted is also incorrect. The government relies heavily on two cases in which courts upheld suspicionless searches of electronic devices, but those cases are not binding on this Court, do not address prolonged detention and searches, and their reasoning is in substantial tension with Second Circuit and Supreme Court jurisprudence. *Compare United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008), *and United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), *with United States v. Ramsey*, 431 U.S. 606 (1977), *and United States v. Irving*, 452 F.3d 110 (2d Cir. 2006). The DHS policies violate the Fourth Amendment because electronic device searches are "non-routine" searches for which reasonable suspicion is required; because searches of expressive material require more procedural protections, *Roaden v. Kentucky*, 413 U.S. 496, 501-04 (1973), which the current policies do not provide; and because the searches are particularly offensive in manner, *Ramsey*, 431 U.S. at 618 n.13. The policies also violate the Fourth Amendment because they permit the suspicionless detention and continued searching of travelers' information after travelers have left the border. As a search and seizure becomes more removed in time and place from the border, a higher level of suspicion is required. *United States v. Stewart*, 715 F. Supp. 2d 750, 753-54 (E.D. Mich. 2010). Moreover, the DHS policies violate the First Amendment because the boundless search and detention of information contained in travelers' electronic devices triggers heightened scrutiny, which a suspicionless search regime cannot satisfy. *Tabbaa*, 509 F.3d at 102; *see Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963).

Finally, Mr. Abidor's claim for a declaration that the May 2010 search of his electronic devices was unconstitutional should not be dismissed because, for the reasons stated above, the suspicionless search and detention of his electronic devices violated his Fourth and First Amendment rights. Moreover, the cumulative effect of the search and detention violated his Fourth Amendment rights. *Tabbaa*, 509 F.3d at 99.

I. PLAINTIFFS HAVE STANDING.

To have standing, plaintiffs must establish (1) that they have suffered a "concrete and particularized" injury that is "actual or imminent"; (2) there is a causal connection between their injury and the challenged statute or conduct, such that the injury is "fairly traceable" to the defendant's alleged violation; and (3) it is "likely" that their injury would be redressed by a favorable decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). Plaintiffs meet each of these criteria.

Contrary to defendants' contention that plaintiffs have failed to satisfy the injury-in-fact requirement, plaintiffs have demonstrated two distinct injuries, each of which is independently sufficient to satisfy Article III. First, plaintiffs have demonstrated an actual and well-founded fear that their electronic devices will be searched and detained in the future under the policies. Second, they have demonstrated that the policies have already caused them concrete injury. Moreover, Mr. Abidor has standing because he seeks expungement of data he believes that DHS has retained as a result of its searches.

A. Plaintiffs Have Standing Because Of The Threat Of Future Injury.

Plaintiffs have established injury-in-fact based on the threat that their or their members' electronic devices will be searched and detained pursuant to the policies in the future. When plaintiffs allege a First Amendment injury based on the fear of future harm, they must show that the fear is "actual and well-founded." *Am. Booksellers Found. v.*

Dean, 342 F.3d 96, 101 (2d Cir. 2003). For Fourth Amendment claims, plaintiffs must show a "realistic danger of sustaining a direct injury." *Pennell v. San Jose*, 485 U.S. 1, 7-8 (1988) (internal quotation marks omitted). While past harm alone does not establish a future injury, "past wrongs are evidence bearing on whether there is a real and immediate threat of repeated injury." *O'Shea v. Littleton*, 414 U.S. 488, 495-96 (1974).

Plaintiffs satisfy these requirements, for three reasons:

First, it is undisputed that the conduct plaintiffs challenge—the suspicionless search and retention of electronic devices—is expressly authorized by official policies promulgated by defendants. Compl. ¶¶ 13-19. The fact that the "alleged risk of harm arises from an established government policy" is a "critical factor[] that weigh[s] in favor of concluding that standing exists." *Baur*, 352 F.3d at 637.[2]

[2] Defendants rely on *City of Los Angeles v. Lyons*, 461 U.S. 95 (1983), but the existence of an official policy sanctioning the conduct plaintiffs challenge distinguishes this case from *Lyons*. In *Lyons*, the plaintiff alleged that his constitutional rights were violated when police officers stopped him for a traffic violation and, without provocation or justification, seized him and applied a chokehold that rendered him unconscious. *Id.* at 97-98. According to the Court, "[i]n order to establish an actual controversy in this case, Lyons would have had not only to allege that he would have another encounter with the police, but also to make the incredible assertion either, (1) that *all* police officers in Los Angeles *always* choke any citizen with whom they happen to have an encounter, whether for the purposes of arrest, issuing a citation or for questioning or, (2) that the City ordered or authorized police officers to act in such manner." *Id.* at 105-06. Here, unlike in *Lyons*, the policy is "authorized." CBP and ICE have issued official policies authorizing the suspicionless search and detention of electronic devices. Compl. ¶ 1. *Lyons* is inapplicable for a second reason. In *Lyons*, the Supreme Court found that there was no concrete controversy in part because in order to be again at risk of being put in a chokehold, *Lyons* would have to break some law—a law which he was *not* challenging—in order to be subjected to the action he contended was illegal. 461 U.S. at 106. In this case, plaintiffs would not have to violate any law in order to face the threat that they would again be subjected to the suspicionless search or detention of their devices. They would merely have to be traveling internationally. Accordingly, unlike in *Lyons*, plaintiffs here face a credible threat of future injury. *See LaDuke v. Nelson*, 762 F.2d 1318, 1326 (9th Cir. 1985) (noting that plaintiffs have standing because they "are subject to constitutional injury based on . . . completely innocent behavior.").

Second, plaintiffs are part of the class targeted by the policies they challenge, which courts have found sufficient to establish standing. In the context of drug testing policy cases, individuals who might be subject to drug testing have standing to challenge the policies, even where the policies involved random or suspicionless testing. *See, e.g.*, *Cronin v. FAA*, 73 F.3d 1126, 1130 (D.C. Cir. 1996); *Amalgamated Transit Union v. Skinner*, 894 F.2d 1362, 1366 (D.C. Cir. 1990). As part of the class of international travelers targeted by the government's suspicionless search and detention policies, plaintiffs have standing to challenge these policies.

Third, plaintiffs have demonstrated an adequate probability of future injury. "[T]he courts of appeals have generally recognized that threatened harm in the form of an increased risk of future injury may serve as injury-in-fact for Article III standing purposes." *Baur*, 352 F.3d at 633 (collecting cases). *Baur* recognized the increased probability of harm in that case as sufficient to confer standing, and cited other cases where the Second Circuit had done the same. *Id.* at 634. "Even a small probability of injury is sufficient to create a case or controversy—to take a suit out of the hypothetical—provided of course that the relief sought would, if granted, reduce the probability." *Vill. of Elk Grove v. Evans*, 997 F.2d 328, 329 (7th Cir. 1993). Courts have found standing based on the risk of fire of 1 in 10,000 wells per year, *Sierra Club v. Mainella*, 459 F. Supp. 2d 76, 93 (D.D.C. 2006), or of a lifetime risk of nonfatal skin cancer of about 1 in 200,000, *NRDC v. EPA,* 464 F.3d 1, 7 (D.C. Cir. 2006).

Plaintiffs have alleged facts sufficient to show that there is an adequate probability of future injury. Not only are plaintiffs or their members part of a class targeted by a policy, but they are also more likely to be searched than others, because of

where they travel and with whom they interact. At least 50 NACDL members currently or have previously represented terrorism suspects, and have had to travel internationally to meet with witnesses and others. Compl. ¶ 70. Similarly, NPPA members frequently travel overseas to report on violent conflicts and international crime, reportage that brings them into contact with individuals of interest to the U.S. government. *Id.* ¶ 103. Moreover, Mr. Abidor, as a Ph.D. student in Islamic Studies, will continue to travel to the Middle East and elsewhere to pursue his studies. Given that Mr. Abidor has reason to believe that the government has searched his electronic devices twice already—once in May 2010 and again in December 2010, Ex. A ¶ 7—he is likely to be searched again in the future.[3] Finally, far from an isolated incident, plaintiffs' Complaint alleges that between October 1, 2008 and June 2, 2010, over 6,500 people had their electronic devices searched at the border, and 220 electronic devices were detained. Compl. ¶ 20.

Two of the plaintiffs are large membership organizations suing on behalf of their members. To satisfy the requirements of associational standing, these plaintiffs need to establish only that at least one member has standing in his or her own right. *Bldg. & Constr. Trades Council of Buffalo v. Downtown Dev., Inc.*, 448 F.3d 138, 145 (2d Cir. 2006). In a case in which organizations brought a pre-enforcement challenge to a state voting registration statute they argued had the chance of disenfranchising their members, the Eleventh Circuit found standing by reasoning that where membership organizations

[3] Defendants also highlight that the searches of the NACDL and NPPA members took place "before the challenged policies were issued." Defs.' Br. 16. But that is of no moment. What plaintiffs challenge is the suspicionless search and detention of electronic devices at the border. The policies described in the complaint currently authorize such searches and detentions, but, as explained above, *see supra* page 6, they replaced earlier policies that authorized substantially the same actions. A contrary rule would mean that government agencies could avoid answering for their policies simply by relabeling them.

"collectively claim around 20,000 members state-wide, it is highly unlikely—even with only a one percent chance of rejection for any given individual—that not a single member will have his or her application rejected." *Fla. State Conference of NAACP v. Browning*, 522 F.3d 1153, 1163 (11th Cir. 2008). Given where NACDL and NPPA members travel and who they talk to, it is "highly unlikely" that "not a single member" will have his or her electronic devices searched or detained pursuant to the policies.

Rather than contesting the adequacy of the jurisdictional facts in plaintiffs' Complaint, defendants have submitted an affidavit stating that CBP "encountered" about 590 million inbound travelers between October 1, 2008 and June 2, 2010. Defs.' Br. Ex. D ¶ 4. Defendants use this figure to argue that "there was only one [electronic device] search for every 90,000 inbound travelers." Defs.' Br. 16. This statistic does not undercut the reasonableness of plaintiffs' fear of suspicionless searches in the future. Plaintiffs allege that the DHS policies authorize *suspicionless* searches, not that electronic device searches are *random*. Some individuals are more likely to be searched than others. Mr. Abidor has reason to believe he has already been searched twice. Moreover, a 12-year-old child with a laptop is presumably far less likely to be searched than an NACDL member who has met with those of interest to the U.S. government.[4]

B. Plaintiffs Have Standing Because They Have Already Suffered "Specific Present Objective Harm."

Plaintiffs also satisfy the injury-in-fact requirement by showing that the policies have caused them to suffer concrete injuries. Plaintiffs have had to take objectively reasonable, burdensome steps to mitigate the policies' harms. Mr. Abidor has reduced

[4] If this Court finds that defendants' declaration calls plaintiffs' standing into doubt, it should permit discovery into the frequency of electronic devices searches and detentions and how travelers are singled out for them. *See Alliance for Envtl. Renewal, Inc.*, 436 F.3d at 87-88 (district courts have discretion to permit discovery into jurisdictional facts).

the amount of information on his computer, self-censors what he downloads, changed the way he does research when abroad so as to avoid taking notes except when absolutely necessary, and intends to warn those he interviews that his notes and any documents they provide him may be reviewed by the U.S. government. Compl. ¶¶ 62-64. Members of NACDL, ethically bound to preserve the attorney-client and other legal privileges, refrain from taking notes or making recordings of certain meetings while abroad. *Id.* ¶ 83. Some members of NPPA no longer guarantee confidentiality to interviewees. *Id.* ¶ 117.

To serve as the basis for standing, presently occurring injuries must be a "specific present objective harm." *Laird v. Tatum*, 408 U.S. 1, 13-14 (1972). Injury can be based on objectively reasonable prophylactic measures a person takes to avoid future injury. *See, e.g.*, *Friends of The Earth, Inc. v. Laidlaw Envtl. Servs.*, 528 U.S. 167, 184-85 (2000); *Williams v. Town of Greenburgh*, 535 F.3d 71, 78 (2d Cir. 2008) (chill to speech can confer standing); *Presbyterian Church v. United States*, 870 F.2d 518 (9th Cir. 1989); *Ozonoff v. Berzak*, 744 F.2d 224, 229-230 (1st Cir. 1984). The legal question is whether the harm is "objective" or "reasonable." *Laidlaw*, 528 U.S. at 184. In *Laidlaw*, the Court found plaintiffs had standing because the challenged conduct was already occurring, and hence "the only 'subjective' issue [was] '[t]he reasonableness of [the] fear' that led the affiants to respond to that concededly ongoing conduct by refraining from use of the North Tyger River and surrounding areas." *Id.* The Court found "nothing 'improbable' about the proposition that a company's continuous and pervasive illegal discharges of pollutants into a river would cause nearby residents to curtail their recreational use of that waterway and would subject them to other economic and aesthetic harms." *Id.* at 184-85.

As in *Laidlaw*, plaintiffs challenge conduct that is already occurring. The policies exist and have already been applied to plaintiffs or their members. There is nothing improbable or unreasonable about plaintiffs taking steps to protect their devices.[5]

C. Plaintiff Abidor Has Standing Because He Seeks Expungement.

Finally, Mr. Abidor has standing for the additional reason that he seeks expungement of information he believes DHS may have retained from his electronic devices. Compl. ¶ 54; CBP Policy § 5.4.1.2 (permitting retention); ICE Policy § 8.5(1)(b) (same). This is an ongoing injury, and the Second Circuit has recognized that plaintiffs possess standing based on a demand for expungement. *Tabbaa*, 509 F.3d at 96 n.1.

II. THE POLICIES VIOLATE THE CONSTITUTION.

This Court should not dismiss plaintiffs' challenge because defendants' policies violate both the Fourth and First Amendments. The policies purport to authorize the government to engage in purely suspicionless searches of the contents of travelers' electronic devices. Because of the highly personal and private nature of the content of people's electronic devices, such searches violate the Fourth Amendment in the absence of at least reasonable suspicion because they are "non-routine" searches, because they are searches of expressive material, and because of the particularly offensive manner in which they are carried out. Moreover, this Court should hold that the policies are unconstitutional because they allow the government to detain electronic devices at the border and continue to search them, without any limitations on how long or what the

[5] NACDL members are ethically bound to take such precautions. Compl. ¶ 83. Similarly, NPPA members have a professional obligation to safeguard the confidentiality of their sources, *id.* ¶¶ 111-14, and therefore must take steps to avoid the harm that would be caused by a border search of their electronic devices, *id.* ¶ 116.

government may search. Furthermore, the policies also violate the First Amendment because searches of private expressive material trigger heightened scrutiny, which the suspicionless and limitless searches that the policies authorize cannot meet.

A. The Policies Violate The Fourth Amendment.

1. The Policies Violate The Fourth Amendment Because They Allow Suspicionless Searches Of Travelers' Electronic Devices.

The Fourth Amendment prohibits the government from searching the contents of electronic devices at the border absent reasonable suspicion, for three reasons. First, because of their invasive nature, searches of electronic devices are "non-routine" searches that require reasonable suspicion. Second, because electronic device searches involve searches of First Amendment-protected material, the reasonable suspicion standard is the constitutional minimum. Finally, electronic device searches are unreasonable because of the "particularly offensive manner" in which they are carried out.

a. Searches Authorized By The Policies Are Not Routine.

The border is not a Fourth Amendment-free zone. Although the Supreme Court has found that the government has broad powers to conduct searches at the border, *see Ramsey*, 431 U.S. at 616, it has also recognized that "non-routine" border searches require at least reasonable suspicion of wrongdoing, *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985). The Second Circuit has held that when deciding whether a search is non-routine, "[t]he determining factor is . . . 'the level of intrusion into a person's privacy.'" *Tabbaa*, 509 F.3d at 98 (quoting *Irving*, 452 F.3d at 123). Defendants are wrong to suggest that searches of property are always routine and that only searches of persons can qualify as non-routine. In *Tabbaa*, the court held that

"intrusive questioning, photographing, and fingerprinting" is "near the outer limits of what is permissible absent reasonable suspicion." 509 F.3d at 98-99.

If "intrusive questioning" pushes the boundaries of what the government can do absent reasonable suspicion, then surely searching and reading through the contents of vast quantities of personal and expressive information contained on someone's electronic devices triggers the reasonable suspicion requirement. Electronic device searches are even more intrusive than questioning because questioning leaves to the traveler the decision of how granular an answer to provide. For example, a traveler may answer a question by saying "I traveled to Montreal" whereas the computer would "answer" the same question by providing a complete itinerary, emails with friends in Montreal, dinner and hotel reservations, and photographs. The nature of the documents the government reviewed when it searched through Mr. Abidor's computer—conversations with his girlfriend, his personal photos, his tax returns, and more—illustrates the intrusive nature of electronic device searches. Compl. ¶ 51.

An electronic device search intrudes upon a traveler's dignity and privacy. With each passing day, people conduct and store more of their lives on computers, smart phones, and other devices. These devices are far more than receptacles for private files; they have become a commonplace part of the daily life of the average person. They are constantly used to help people think, learn, communicate, associate with others and keep track of their own lives and those of their families. *See generally* Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 Widener L.J. 667 (2006). A consequence of this new reality is that these devices also maintain a nearly indelible record of everything their users think or search for, what they learn or read, what they say to others, and with whom

they associate. It should therefore come as no surprise that "for most people, their computers are their most private spaces." *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting).

Computers are the gateway to the Internet and all it has to offer, including means of communicating through e-mail, instant messaging, and social networks. As the Sixth Circuit recently noted in holding that individuals have a right to privacy in email:

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities. Much hinges, therefore, on whether the government is permitted [access to] a subscriber's emails without triggering the machinery of the Fourth Amendment.

United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010). Suspicionless searches of electronic devices that facilitate, record, and store such communications undoubtedly implicate heightened concerns of privacy and dignity that distinguish the devices from other types of property that travelers may carry across the border.

The uniquely private and vast quantity of information contained on personal computers magnifies the privacy and dignity concerns implicated by a border search. A computer "is akin to a vast warehouse of information," and a typical hard drive sold in 2005 can carry data "roughly equivalent to forty million pages of text—about the amount of information contained in the books on one floor of a typical academic library." Orin S.

Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1175 (9th Cir. 2010) ("[E]ven inexpensive electronic storage media today can store the equivalent of millions of pages of information."). Such a vast quantity and variety of information increases the likelihood that highly personal information will also be searched, seized or copied. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 104 (1994). As a consequence, individuals' privacy and dignity interests in the contents of their laptops more closely resemble the heightened interests associated with private dwelling areas and should be treated accordingly. *Cf. United States v. Whitted*, 541 F.3d 480, 488 (3d Cir. 2008) (requiring suspicion for search of passenger cabin of a vessel).

Defendants attempt to minimize the privacy interests at stake by arguing, sweepingly, that a border search is always routine unless it involves an invasive bodily search. They seize on *United States v. Flores-Montano* to suggest, incorrectly, that if the search of a vehicle's fuel tank does not implicate the same dignity and privacy interests as a "highly intrusive search[] of the person," 541 U.S. 149, 152 (2004), then there must be no property search capable of implicating those interests. Defs.' Br. 19. But the Court in *Flores-Montano* specifically limited its holding to vehicles. It certainly did not hold that all property searches are routine or that they are categorically incapable of implicating the "dignity and privacy interests of the person being searched." 541 U.S. at 152; *see also Whitted*, 541 F.3d at 489; *United States v. Alfonso*, 759 F.2d 728, 738 (9th Cir. 1985) (finding that a border search of the private living quarters on a ship "should require something more than naked suspicion").

Defendants also wrongly rely on the closed container doctrine for support, likening laptops to luggage. Defs.' Br. 23. Laptops are not like luggage. While both are capable of storing personal items, the similarity stops there. Far from a glorified suitcase, a personal computer is a revolutionary and indispensible communications tool, allowing users to instantly exchange ideas via e-mail, instant messenger services, blogs, chat rooms, and social networks. It is also the interface that allows people to read and publish information on the Internet covering a range of topics "as diverse as human thought." *Reno v. ACLU*, 521 U.S. 844, 863 (1997) (The Internet "is the most participatory form of mass speech yet developed, entitled to the highest protection from governmental intrusion."). In addition, it is nearly impossible to effectively remove private information from electronic devices in the same way that one could leave a sensitive file at home or take it out of a briefcase prior to crossing the border. When a computer file is deleted, the underlying data remains on the hard drive until it is overwritten at some unknown point in the future. Even partially overwritten files can be recovered by computer forensic experts. *Gourde*, 440 F.3d at 1068; s*ee generally* Kerr, 119 Harv. L. Rev. at 542 ("Computers are also remarkable for storing a tremendous amount of information that most users do not know about and cannot control"). This problem is compounded by the fact that computers routinely store information without the user's knowledge, creating a searchable, retrievable log that reveals the precise details of an individual's reading and viewing habits. Any comparison to a mere closed container vastly oversimplifies a computer's functions and simply ignores the realities of modern existence.

b. Searches Authorized By The Policies Burden Expressive Interests.

Electronic device searches invariably involve examining an extensive amount of expressive material. When a search or seizure burdens expressive interests, those interests must be considered in determining whether the search or seizure is reasonable. Because they implicate expressive interests, conducting electronic device searches and seizures in the absence of suspicion is unreasonable and violates the Fourth Amendment.

Not all searches and seizures are the same; "[a] seizure reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material." *Roaden*, 413 U.S. at 501. As *Roaden* held, seizures of expressive materials, such as "books and movie films," are "to be distinguished from" seizures of "instruments of a crime" or "contraband" in appraising reasonableness. *Id.* at 502. Examining reasonableness "in light of the values of freedom of expression," the Court required police to obtain a warrant to seize expressive materials even though one would not otherwise have been required. *Id.* at 504.

Searches that implicate expressive materials therefore require the application of heightened Fourth Amendment requirements, up through and including a warrant and probable cause, even where those requirements might not otherwise apply. *Id.* at 501-04; *see also Maryland v. Macon*, 472 U.S. 463, 468 (1985) ("First Amendment imposes special constraints on searches for and seizures of presumptively protected material."); *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326 n.5 (1979) (same).[6] Relatedly, the

[6] To be clear, the meaning of the *probable cause* requirement remains the same whether or not a search targets expressive materials. *New York v. P.J. Video, Inc.*, 475 U.S. 868, 873-75 & n.6 (1986). But as the cases cited in this paragraph make clear, where a search and seizure burdens expressive interests, those interests must be taken into account in determining what protections are necessary to make the search reasonable.

Fourth Amendment's procedural protections must be applied with "scrupulous exactitude" when a search implicates expressive materials. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *see also United States v. U.S. District Court (Keith)*, 407 U.S. 297, 317 (1972); *Stanford v. Texas*, 379 U.S. 476, 485 (1965); *Marcus v. Search Warrants*, 367 U.S. 717, 729 (1961). Because searching electronic devices implicates expressive interests, more procedural protections are required than may typically apply to non-expressive materials searched at the border. While these cases did not involve the border, the Supreme Court has repeatedly rejected the proposition that the border is a Fourth Amendment-free zone, *see, e.g.*, *Montoya de Hernandez*, 473 U.S. at 537-38, and has suggested that government intrusions that implicate expressive conduct, even at the border, should be policed especially carefully by courts, *see, e.g.*, *Ramsey*, 431 U.S. at 624 n.18 (suggesting that "full panoply of Fourth Amendment requirements" might be applicable where government searches implicate expressive rights or threaten to "chill" expressive conduct (citing, *inter alia*, *Roaden* and *Stanford*)). In short, searching electronic devices is different than searching ordinary luggage, and a traveler does not lose her right to privacy in expressive materials simply because she crosses the border. *Cf. Lamont v. Postmaster Gen.*, 381 U.S. 301, 305 (1965) (holding that restrictions on unfettered delivery of mail from abroad infringed addressees' First Amendment rights).

c. Searches Authorized By The Policies Are Particularly Offensive In Manner.

Finally, reasonable suspicion is required because of the particularly offensive manner in which electronic device searches are carried out. In *Ramsey*, the Supreme Court stated that a border search may be constitutionally objectionable "because of the particularly offensive manner in which it is carried out." 431 U.S. at 618 n.13. Citing to

cases in which the Court had limited the extent to which the government could conduct broad-ranging searches or seizures incident to arrest, the Court suggested that the offensiveness of the execution of a search may violate the Constitution. *Id.* (citing, *e.g.*, *Kremen v. United States*, 353 U.S. 346, 347 (1957) ("The seizure of the entire contents of the house and its removal some two hundred miles away to the F.B.I. offices for the purpose of examination are beyond the sanction of any of our cases.")). Laptop searches, too, are inherently offensive in manner. As described above, *see supra* Part II.A.1.a, electronic devices contain vast quantities of deeply personal and sensitive information. The policies authorize the government to search this information without any limits on the search's duration, subject matter, or scope. Limiting searches to where the government can meet the reasonable suspicion standard is the best means to reconcile the privacy interests of travelers with the government's need to enforce the law at the border.

2. The Policies Violate The Fourth Amendment Because They Permit The Suspicionless And Indefinite Detention And Search Of Electronic Devices And The Information They Contain.

This Court should further hold that defendants' policies violate the Fourth Amendment because they purport to authorize the government to detain electronic devices and search them after a traveler has left the border, absent reasonable suspicion. Even at the border, the Fourth Amendment does not sanction suspicionless and lengthy—let alone indefinite—detentions. *See Montoya de Hernandez*, 473 U.S. at 539-41.

As searches and seizures become removed in time and place from the border, a higher level of suspicion is required. The extended border search doctrine governs searches occurring when "a person or some property has cleared an initial customs checkpoint and [has] entered the United States." *United States v. Gaviria*, 805 F.2d

1108, 1112 (2d Cir. 1986) (internal quotation marks omitted). Because such a search is a "greater intrusion on legitimate expectations of privacy, [it is] permitted only if supported by reasonable suspicion." *Id.* (internal quotation marks omitted).

A number of lower courts, most applying this extended border search doctrine, have held that CBP must have reasonable suspicion or probable cause before seizing a laptop at the border, transporting it elsewhere, and searching it at a later time. *See, e.g.*, *United States v. Hanson*, No. CR 09-00946, 2010 WL 2231796 (N.D. Cal. June 2, 2010) (a laptop search occurring 9-17 days after border seizure in another location required reasonable suspicion; a search occurring a few months later required probable cause); *Stewart*, 715 F. Supp. 2d 750 (a search 24 hours after seizure in a location away from the border required reasonable suspicion); *United States v. Laich*, No. 08-20089, 2010 WL 259041 (E.D. Mich. Jan. 20, 2010) (a permanent seizure of a laptop at the airport, and its transportation hundreds of miles away, required probable cause); *United States v. Cotterman*, No. CR 07-1207, 2009 WL 465028 (D. Ariz. Feb. 24, 2009); *see also United States v. Rogozin*, No. 09-CR-379, 2010 WL 4628520, at *4-5 (W.D.N.Y. Nov. 16, 2010) (Report and Recommendation). Courts of Appeals have also held that as a border detention and search become prolonged, a higher level of suspicion—and eventually, a warrant based on probable cause—becomes necessary. *See, e.g.*, *United States v. Yang*, 286 F.3d 940, 948 (7th Cir. 2002); *United States v. Caicedo-Guarnizo*, 723 F.2d 1420, 1423 (9th Cir. 1984).

In a distinct line of authority, the Supreme Court has made clear that investigatory detentions are subject to reasonable temporal limits. In *United States v. Place*, the Court held that the detention of a domestic traveler's luggage for 90 minutes without probable

cause violated the Fourth Amendment. 462 U.S. 696, 699, 708-10 (1983). The Court held that the length of the detention is "an important factor" in determining whether a seizure is reasonable. *Id*. In *Montoya de Hernandez*, the Supreme Court applied this duration principle in assessing the reasonableness of a border search. 473 U.S. at 542-44. In considering whether a 16-hour border detention could be justified only by reasonable suspicion, the Court in *Montoya de Hernandez* similarly analyzed, citing twice to *Place*, "whether the detention of [the] respondent was reasonably related in scope to the circumstances which justified it initially." *Id*.[7]

Although the government relies on *United States v. Gaviria* for the proposition that the extended border search doctrine is inapplicable here, *Gaviria* involved an entirely different context—the shipment of goods—and focused on whether the destination customs station was "the 'functional equivalent' of the international border," a concept distinct from the "'extended border.'" 805 F.2d at 1112. Moreover, *Gaviria* specifically "endeavored to sustain Customs' established practice of conducting routine border searches at the customs station closest to the final destination of the goods." *Id*. at 1113.

The extended detention of electronic devices carried by a traveler poses a very different set of concerns. *See Place*, 462 U.S. at 708 ("Particularly in the case of detention of luggage within the traveler's immediate possession, the police conduct intrudes on both the suspect's possessory interest in his luggage as well as his liberty interest in proceeding with his itinerary."). *Place* and *Montoya de Hernandez* make clear that the length and scope of a detention must be reasonably related to its initial

[7] Although *Montoya de Hernandez* involved a person, *Place* concerned "detention of luggage within the traveler's immediate possession" and rejected the idea that "seizures of property are generally less intrusive than seizures of the person." 462 U.S. at 708-09.

justification. The extended border search doctrine was developed precisely to distinguish between routine searches closely linked to a border crossing and limited in both scope and duration, and more invasive and lengthier searches and detentions for which a requirement that the government demonstrate reasonable suspicion is both reasonable and practical. *See, e.g.*, *United States v. Abbouchi*, 502 F.3d 850, 855 (9th Cir. 2007) ("Because 'the delayed nature of an extended border search . . . necessarily entails a greater level of intrusion on legitimate expectations of privacy than an ordinary border search,' the government must justify an extended border search with reasonable suspicion that the search may uncover contraband or evidence of criminal activity." (quoting *Caicedo-Guarnizo*, 723 F.2d at 1422); *Stewart*, 715 F. Supp. 2d at 754. This is common sense; as a detention becomes lengthier, it becomes more invasive, aggravating flaws already present in electronic device searches even as concerns of urgency, any relationship to the border, and the impracticality of getting a warrant recede. *See Laich*, 2010 WL 259041, at *4. Lower courts, as discussed above, have held that electronic device searches occurring just one to two days after an initial seizure at the border required reasonable suspicion or probable cause. A border search of a traveler's electronic devices simply cannot be expanded beyond standard temporal and locational limits without becoming an "extended border search" requiring reasonable suspicion.

Defendants' justification of their policies' authorization of lengthy, suspicionless detentions on the ground that searching electronic files "can take a long time" is meritless. Defs.' Br. 24-25. The cases to which defendants cite, which as defendants acknowledge involved searches pursuant to warrants, do not speak to whether such lengthy, invasive searches may be conducted in the absence of a warrant, let alone in the

absence of any suspicion. In-depth computer searches take time precisely because they are so invasive, involving numerous unrelated pieces of personal information. *Cf. United States v. Hill*, 459 F.3d 966, 968 (9th Cir. 2006) ("[B]ecause computers typically contain so much information beyond the scope of the criminal investigation, computer-related searches can raise difficult Fourth Amendment issues different from those encountered when searching paper files."). They invade individuals' privacy and infringe their ability to conduct their livelihoods and communicate with others. *See id.* at 976 n.12 ("For some people, computer files are the exclusive means of managing one's life—such as maintaining a calendar of appointments or paying bills. Thus, there may be significant collateral consequences resulting from a lengthy, indiscriminate seizure of all such files."). The length of these potentially limitless invasions, moreover, typically vastly exceeds the several-hour detentions that *Tabbaa* suggested were towards the outer limits of "routine." *See* 509 F.3d at 100-01. Because the policies authorize detentions of unlimited length in the absence of any suspicion even after a traveler leaves the border, they cannot satisfy the "reasonable relationship" requirement. They therefore violate the Fourth Amendment.

B. The Policies Violate The First Amendment.

The government gives short shrift to plaintiffs' First Amendment challenge, stating only that a search that satisfies the Fourth Amendment cannot violate one's First Amendment rights. But in addition to the argument that Fourth Amendment requirements are heightened when a search and seizure implicates the First Amendment, *see supra* Part II.A.2, plaintiffs raise an independent First Amendment claim against the policies that authorize the search and detention of electronic devices at the border.

Searches and detentions at the border "can constitute a direct and substantial interference" with First Amendment rights. *Tabbaa*, 509 F.3d at 101; *see also Lamont*, 381 U.S. at 305. In *Tabbaa*, plaintiffs were searched and detained at the border based on having attended an Islamic conference in Canada. Concluding that the government's actions significantly burdened plaintiffs' First Amendment associational rights, the Second Circuit applied strict scrutiny to those actions. 509 F.3d at 102. The court emphasized that the question of whether the searches "constituted a significant or substantial burden on plaintiffs' First Amendment associational rights" was entirely distinct from whether the search passed muster under the Fourth Amendment. *Id*. at 102 n.4.

Individuals have a right to engage in First Amendment activity in private; government intrusions into that privacy trigger heightened scrutiny. *See NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958) ("[I]nviolability of privacy in group association may in many circumstances be indispensible to preservation of freedom of association, particularly where a group espouses dissident beliefs."); *see also Brown v. Socialist Workers '74 Campaign Comm.*, 459 U.S. 87, 91-93 (1982); *Shelton v. Tucker*, 364 U.S. 479, 488 (1960); *Bates v. City of Little Rock*, 361 U.S. 516, 524 (1960). More specifically, where a government investigation treads on First Amendment interests, the government must demonstrate a compelling need and substantial relation between that need and the information sought to proceed. *See Gibson*, 372 U.S. at 546 ("[I]t is an essential prerequisite to the validity of an investigation which intrudes into the area of constitutionally protected rights of speech, press, association and petition that the State convincingly show a substantial relation between the information sought and a subject of

overriding and compelling state interest."); *Watkins v. United States*, 354 U.S. 178, 197 (1957).

Because they burden the right to engage in First Amendment activity in private, lower courts have applied heightened scrutiny to efforts to find out what individuals are reading or what movies they are watching. *See, e.g.*, *Amazon.com LLC v. Lay*, No. C10-664, 2010 WL 4262266, at *10-12 (W.D. Wash. Oct. 25, 2010) (holding that state's request for titles of expressive materials purchased through Amazon.com violated customers' First Amendment rights); *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*, 706 F. Supp. 2d 11, 17 (D.D.C. 2009); *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 572 (W.D. Wis. 2007); *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, No. 98-MC-138, 26 Med. L. Rptr. 1599, 1600 (D.D.C. Apr. 6, 1998).

Just as heightened scrutiny applies to government efforts to compel disclosure of records of sales of expressive items, testimony about one's beliefs, or an association's membership list, it must apply to government attempts to search individuals' electronic devices. Searching electronic devices at the border forces individuals to reveal their thoughts where those thoughts had previously been shielded from observation, interfering with free expression. Indeed, electronic devices searches often reveal a greater wealth of expressive materials than the searches considered in past cases; a single such device can and frequently does contain private writings, correspondence, research, records of movie and TV viewing and reading habits, personal photographs and videos, a log of recently visited websites, tax and financial records, job applications, and the like. The search of Mr. Abidor's electronic devices illustrates the point: the government read his personal

correspondence, academic writings and research. Compl. ¶ 51. Because searches of such devices are so invasive of individual privacy—as invasive, if not more so, than a search of one's home or office, and certainly more invasive than a subpoena for book or movie titles—the First Amendment demands protections as strong as those that attach to other government activities that have an impact on speech and associational rights.

The infringement is unconstitutional unless it "serves compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive" of First Amendment freedoms. *Tabbaa*, 509 F.3d at 102 (quoting *Roberts v. United States Jaycees*, 468 U.S. 609, 623 (1984)); *see also Gibson*, 372 U.S. at 546 (requiring that "the State convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest"). Yet against the strong interests in individual privacy that plaintiffs identify, the government offers only general interests in policing the border.

These interests are not sufficient to sustain the challenged policies. However strong the government's interests may be, the policies cannot satisfy the "substantial relation" or "significantly less restrictive means" requirements because the policies do not require any articulable suspicion. The electronic device search policies at issue here permit the government to search the devices of any individual seeking to cross the border, for any reason, in the absence of any suspicion. That alone would be enough to make them not narrowly tailored to the government's asserted interest here. Moreover, because the large storage capacity of today's electronic devices allows them to hold a vast array of expressive information accumulated over a period of time, typically much of the information on a given U.S.-based traveler's laptop or smartphone will have little or no

relationship to activities conducted abroad. This makes it impossible to show a "substantial relation" between governmental interests in examining the devices and in policing the border.

The government relies on *United States v. Borello*, 766 F.2d 46 (2d Cir. 1985), for the proposition that electronic device searches do not implicate the First Amendment, but that stretches the case too far. Although the defendant in *Borello* was convicted for making false statements and smuggling in connection with the shipment and importation of five cartons containing 771 pornographic films, he argued that he was being prosecuted in violation of the First Amendment because he was "tried and sentenced for importing adult films without any determination that the materials were legally obscene." *Id*. at 58. The Second Circuit noted that the Supreme Court has long held that the government can block the importation of obscene material, and further noted that "Customs officials can permissibly screen materials entering the country to enforce these laws." *Id*. But the Second Circuit did *not* pass judgment on what standard—reasonable suspicion or something else—the government must meet to engage in such screening. In *Borello*, it was the defendant's failure to properly fill out customs forms that raised border agents' suspicion, triggering examination of the films. *See id.* at 48-50. In addition, *Borello* was decided in an era when a search of a personal electronic device, in the rare instance where one was carried at all, would likely not have implicated the same expressive interests that such a search does today. Nor are the expressive interests at stake otherwise analogous. A traveler has a strong interest in keeping private the contents of a personal laptop and cell phone that she carries across the border, an interest

much greater than that of an importer in keeping the contents of a commercial shipment private.

The generality of the interests articulated, the tenuous connection to the border, and the lack of narrow tailoring, in light of the severe burden that the policies impose on First Amendment rights, means that the policies cannot satisfy heightened scrutiny. They therefore violate the First Amendment and must be struck down.

III. THIS COURT SHOULD NOT DISMISS MR. ABIDOR'S CLAIMS.

Mr. Abidor is entitled to a declaration that the May 2010 search and detention of his electronic devices violated his First and Fourth Amendment rights. For the reasons stated above, the suspicionless search and detention of Mr. Abidor's laptop and external hard drive violated the First and Fourth Amendments. Moreover, Mr. Abidor is entitled to a declaration for an additional reason: the cumulative effect of defendants' searches of Mr. Abidor was more invasive of privacy than that in *Tabbaa*, in which the Second Circuit suggested that in some circumstances the cumulative effect of routine searches can render the entirety of the search non-routine. 509 F.3d at 99. If the "intrusive questioning, photographing, and fingerprinting" in *Tabbaa* were "near the outer limits of what is permissible absent reasonable suspicion," *id.* at 98-99, CBP exceeded that limit when it searched Mr. Abidor. Like the plaintiffs in *Tabbaa*, Mr. Abidor was frisked, questioned extensively, and fingerprinted. In addition, he was handcuffed, removed from the train to the port, kept in a holding cell for a couple of hours, and his electronic devices were extensively searched and detained over a period of eleven days. Compl. ¶¶ 34-46.

CONCLUSION

For the foregoing reasons, the Motion To Dismiss should be DENIED.

Respectfully submitted,

March 9, 2011

/s/ Catherine Crump

Catherine Crump
Hina Shamsi
Benjamin T. Siracusa Hillman
American Civil Liberties Union
Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500

Michael Price
National Association of Criminal
Defense Lawyers
1660 L Street NW, 12th Floor
Washington, D.C. 20036
(202) 872-8600

Christopher Dunn
Melissa Goodman
Arthur Eisenberg
New York Civil Liberties Union
Foundation
125 Broad Street, 19th Floor
New York, NY 10004
(212) 607-3300

CERTIFICATE OF SERVICE

I hereby certify that on March 9, 2011, the foregoing document was filed with the Clerk of the Court and served in accordance with the Federal Rules of Civil Procedure, and/or the Eastern District's Local Rules, and/or the Eastern District's Rules on Electronic Service upon the following parties and participants:

Marcia K. Sowles
Senior Counsel
U.S. Department of Justice, Civil Division
Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7114
Washington, DC 20530
(202) 514-4960
Fax: (202) 616-8470
Email: marcia.sowles@usdoj.gov

Elliot M. Schachner
United States Attorneys Office
Eastern District of New York
271 Cadman Plaza East
Brooklyn, NY 11201-1820
(718) 254-6053
Fax: (718) 254-6081
Email: Elliot.Schachner@usdoj.gov

Attorneys for Defendants Napolitano, Bersin, and Morton

/s/ Benjamin T. Siracusa Hillman
Benjamin T. Siracusa Hillman