UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

PASCAL ABIDOR, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, NATIONAL PRESS PHOTOGRAPHERS ASSOCIATION,

Plaintiffs,

– against –

JANET NAPOLITANO, ALAN BERSIN, JOHN T. MORTON,

Defendants.

**MEMORANDUM & ORDER**

10-CV-04059 (ERK)(JMA)

KORMAN, J.:

> Since the founding of the republic, the federal government has held broad authority to conduct searches at the border to prevent the entry of dangerous people and goods. In the 21st century, the most dangerous contraband is often contained in laptop computers or other electronic devices, not on paper. This includes terrorist materials and despicable images of child pornography.

Michael Chertoff, *Searches Are Legal, Essential*, USA Today, July 16, 2008, at A10.

This case involves a challenge to regulations that were adopted by the Department of Homeland Security ("DHS"), of which Mr. Chertoff was then Secretary, to address and regulate the border searches of laptop computers. Specifically, in August 2009, U.S. Immigration and Customs Enforcement ("ICE") and U.S. Customs and Border Protection ("CBP")—two components of DHS—issued directives that authorize their agents to inspect any electronic devices that travelers seek to carry across an international border into the United States. *See* Defs.' Mot. Dismiss, Ex. A, ICE Directive No. 7-6.1 (Aug. 18, 2009) ("ICE Directive"); Defs.' Mot. Dismiss, Ex. B, CBP Directive No. 3340-049 (Aug. 20, 2009) ("CBP Directive"). These directives authorize the inspection of any files and images stored on electronic devices, the performance of searches on the electronic devices, the detainment of electronic devices for a

reasonable time to perform such searches, and the copying of stored information to facilitate inspection. These activities may be undertaken without reasonable suspicion that the electronic devices contain materials that fall within the jurisdiction of CBP or ICE.

Plaintiffs bring both facial and as-applied challenges to these directives. They allege that the directives purport to authorize unreasonable searches and seizures and operate to chill protected speech. Plaintiffs argue that these searches violate "the constitutional rights of American citizens to keep the private and expressive details of their lives, as well as sensitive information obtained or created in the course of their work, free from unwarranted government scrutiny." Compl. ¶ 3.

They seek a declaratory judgment that the CBP and ICE policies violate the First and Fourth Amendments. Compl. at 34. They also seek a declaration that the defendants violated the rights of Pascal Abidor, the individual plaintiff. Compl. at 34. Along with this declaratory, relief they seek to enjoin defendants from enforcing their policies of searching, copying, and detaining electronic devices at the international border without reasonable suspicion. Compl. at 34. They seek the same relief on Mr. Abidor's behalf. Compl. at 34.

The defendants move to dismiss the complaint. They argue, preliminarily, that the individual plaintiff, Mr. Abidor, and the two plaintiff organizations, the National Association of Criminal Defense Lawyers ("NACDL") and the National Press Photographers Association ("NPPA"), lack standing to bring a facial challenge to the directives. They also argue that plaintiffs' facial and as-applied challenges fail to state a claim upon which relief can be granted. They rest their argument on the Supreme Court's holding in *United States v. Flores-Montano*, 541 U.S. 149 (2004), that "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this

country, are reasonable simply by virtue of the fact that they occur at the border." Defs.' Br. 3 (quoting *Flores-Montano*, 541 U.S. at 152-53 (internal quotation marks omitted)).

## FACTS

### *A. The CBP Directive Authorizing Border Searches of Electronic Devices*

#### 1. Overview

The CBP Directive authorizes CBP officers, "[i]n the course of a border search, with or without individualized suspicion, . . . [to] examine electronic devices and [to] review and analyze the information encountered at the border, subject to the requirements and limitations provided [in the Directive] and applicable law." CBP Directive § 5.1.2; Compl. ¶ 14. The Directive further provides:

> An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days.

CBP Directive § 5.3.1; Compl. ¶ 15. The ICE Directive requires searches of detained electronic devices to be completed "in a reasonable time given the facts and circumstances of a particular search," which will generally be within 30 days. ICE Directive § 8.3(1). If the CBP seizes a traveler's electronic device, the traveler may nonetheless be permitted to enter the country and, if eventually cleared, the device will be sent to the traveler later. CBP Directive § 5.3; Compl. ¶ 16. CBP agents must obtain supervisory approval before they detain an electronic device or make copies of the information contained on it for the purpose of continuing a border search after the traveler leaves the border search site. CBP Directive § 5.3.1.1; Compl. ¶ 16. The ICE Directive does not require supervisory approval before detaining or copying information stored on an electronic device. ICE Directive § 8.2(5).

If the CBP requires technical assistance in order to search the information on the electronic device (for example, if the information is encrypted or written in a foreign language), "[o]fficers may transmit electronic devices or copies of information contained therein to seek technical assistance from other federal agencies, with or without individualized suspicion." CBP Directive § 5.3.2.2; Compl. ¶ 17. If the CBP requires subject-matter assistance in order to "determine the meaning, context, or value of information contained therein," "[o]fficers may transmit electronic devices or copies of information contained therein to other federal agencies for the purpose of obtaining subject matter assistance *when they have reasonable suspicion* of activities in violation of the laws enforced by CBP." CBP Directive § 5.3.2.3 (emphasis added); Compl. ¶ 17. The ICE directive contains a similar reasonable suspicion requirement. ICE Directive § 8.4(2)(b). Seeking either type of assistance requires supervisory approval. CBP Directive § 5.3.2.4. The Directive provides that, unless otherwise necessary, if a traveler's electronic device must be transmitted to another agency, a copy should be made of the information stored on it and the copy transmitted instead of the actual device. CBP Directive § 5.3.2.5.

The Directive provides that copies of information from an electronic device may be retained under certain circumstances:

> Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is *probable cause* to believe that the device, or [a] copy of the contents thereof, contains evidence of or is the fruit of a crime that CBP is authorized to enforce.

CBP Directive § 5.4.1.1 (emphasis added). The Directive specifically requires the destruction of any copies of information contained on a traveler's electronic device:

> Except as noted in section 5.4 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.3, there is *not probable cause* to seize it, any

> copies of the information must be destroyed, and any electronic device must be returned. Upon this determination that there is no value to the information copied from the device, the copy of the information is destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system of records and which must be no later than twenty one (21) days after such determination. The destruction shall be noted in appropriate CBP systems of records.

CBP Directive § 5.3.1.2 (emphasis added); *see also* CBP Directive § 5.3.3.4 ("Except as noted in section 5.4.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the information does not exist, CBP will retain no copies of the information."); CBP Directive § 5.4.1.6 ("Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.").

The Directive permits two categories of information to be retained without probable cause. First, "CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained." CBP Directive § 5.4.1.2. The Directive mentions data collections such as the A-file, Central Index System, TECS, and ENFORCE as possible repositories of such information. *Id.* Second, "CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with elements of the federal government responsible for analyzing terrorist threat information." CBP Directive § 5.4.1.4.

Where the CBP turns an electronic device over to ICE for "analysis and investigation," "ICE policy will apply once it is received by ICE." ICE Directive § 6.2; CBP Directive § 2.7. The CBP Directive requires that, "[a]t the conclusion of the requested assistance, all information must be returned to CBP as expeditiously as possible," and "the assisting federal agency should

destroy all copies of the information transferred to that agency," unless the assisting agency has independent legal authority to do so. CBP Directive §§ 5.4.2.2-5.4.2.3. The ICE Directive contains similar provisions regarding retaining and sharing information, ICE Directive §§ 8.5(1)(a)-(e), and provides as follows regarding destruction:

> Copies of information from electronic devices, or portions thereof, determined to be of no relevance to ICE will be destroyed in accordance with ICE policy governing the particular form of information. Such destruction must be accomplished by the responsible Special Agent within seven business days after conclusion of the border search unless circumstances require additional time, which must be approved by a supervisor and documented in appropriate ICE systems. All destructions must be accomplished no later than 21 calendar days after conclusion of the border search.

ICE Directive § 8.5(e).

**2. Review and Handling of Privileged or Other Sensitive Materials**

Both the CBP and ICE directives contain special provisions relating to the handling of privileged or other sensitive materials. CBP Directive § 5.2; ICE Directive § 8.6. These include legal materials, other possibly sensitive information, "such as medical records and work-related information carried by journalists," as well as business or commercial information. *Id.* Specifically, both directives note that officers "may encounter materials that appear to be legal in nature, or an individual may assert that certain information is protected by attorney-client or attorney work product privilege." CBP Directive § 5.2.1; *see also* ICE Directive § 8.6(2)(b). While such materials do not enjoy a per se exemption from a border search, they are subject to special handling procedures. *Id.* In such circumstances, the CBP Directive provides that, if a CBP officer "suspects that the content of such material may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of the CBP, the Officer must seek advice from the CBP Associate/Assistant Chief Counsel before conducting a search of the

material, and this consultation shall be noted in appropriate CBP systems of records. CBP counsel will coordinate with the U.S. Attorney's Office as appropriate." *Id.*

Other "possibly sensitive" information, "such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy." CBP Directive § 5.2.2; *see also* ICE Directive § 8.6(2)(c). Moreover, CBP officers are advised that "[q]uestions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel, and this consultation shall be noted in appropriate CBP systems of records." CBP Directive § 5.2.2; *see also* ICE Directive § 8.6(2)(c). Finally, "[o]fficers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure." CBP Directive § 5.2.3; *see also* ICE Directive § 8.6(2)(a). Specifically, "[d]epending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information." CBP Directive § 5.2.3; *see also* ICE Directive § 8.6(2)(a).[1]

### *B. The Border Search of Abidor and His Electronic Devices*

On May 1, 2010, Pascal Abidor, a twenty-six-year-old graduate student at the Institute of Islamic Studies at McGill University in Montreal, Canada, was aboard an Amtrak train from Montreal to New York City. Compl. ¶¶ 7, 21, 24. At approximately 11:00 a.m., the train stopped at a United States Customs and Border Patrol inspection point near Service Port-Champlain. Compl. ¶ 25. A CBP officer who inspected Abidor's customs declaration and U.S. passport. Abidor told the CBP officer that he had briefly lived in Jordan and visited Lebanon in

[1] The CBP and ICE directives contain slightly different wording with respect to the sharing of information that is "determined to be protected by law as privileged or sensitive." CBP Directive § 5.2.4; ICE Directive § 8.6(3). The ICE directive provides that such material "is to be handled consistent with the laws and policies governing such information." ICE Directive § 8.6(3). The CBP directive provides that such information "will only be shared with federal agencies that have mechanisms in place to protect appropriately such information." CBP Directive § 5.2.4.

the previous year. Compl. ¶¶ 26-28. While Abidor had obtained visas to these two countries, they were not contained in his United States passport. Instead, they were contained in a French passport which was also in Abidor's possession. Compl. ¶ 28. Abidor was instructed to bring his belongings to the café car for further inspection. Compl. ¶ 29.

Among Abidor's belongings were several electronic devices, including his laptop computer, digital camera, two cellular telephones, and an external computer hard drive. Compl. ¶ 24. The officer removed Abidor's laptop computer from one of his bags, turned it on, and ordered Abidor to enter his password, which he did without objection. Compl. ¶ 30. The officer inspected the laptop, focusing apparently on certain pictures Abidor had saved that depicted rallies of Hamas and Hezbollah, Compl. ¶ 32, both of which were designated by the State Department as terrorist organizations. *See* Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2008, Terrorist Organizations*, U.S. Dep't of State (April 30, 2009), http://www.state.gov/j/ct/rls/crt/2008/122449.htm. When Abidor was asked why he was interested in these images, "Abidor explained that his specific area of research for his Ph.D. degree is the modern history of Shiites in Lebanon," Compl. ¶ 32, in which Hezbollah openly operates. Compl. ¶ 32. Even if this may have explained the pictures of Hezbollah, it did not explain why Abidor saved the pictures of Hamas, a terrorist organization not composed of Shiites and not based in Lebanon.

The CBP officer who was interviewing Abidor "ordered [him] to write down his password [to the laptop]," and Abidor complied. Compl. ¶ 33. Abidor alleges, on information and belief, that his laptop was searched during the five hours from the time he was stopped until he was released. Compl. ¶ 41. In particular, he alleges that at a minimum, one movie and a document related to his dissertation were viewed. Compl. ¶ 41. His laptop was retained by CBP for further inspection by ICE. Compl. ¶ 43. His camera and two cell phones were returned to

him at the border search site. Compl. ¶ 44. "One of his cell phones was returned with a scratch on the back of the phone near the battery, suggesting that someone had tried to open it." Compl. ¶ 44. Abidor's laptop and external drive were returned to him eleven days later by mail. Compl. ¶ 48. It appeared to him that both the laptop and external drive had been physically opened and that various files on the laptop and external drive had been viewed. Compl. ¶ 49.

> Some files opened and examined by the officers included highly private and expressive materials that reveal intimate details about Mr. Abidor's life, such as his personal photos, a transcript of a chat with his girlfriend, copies of email correspondence, class notes, journal articles, his tax returns, his graduate school transcript, and his resume. At the time his laptop was detained, it was configured to automatically allow access to his online email and social networking accounts, raising the possibility that border agents searched through Mr. Abidor's stored correspondence and communications as well.

Compl. ¶ 51. The complaint also alleges on information and belief that one or more agencies copied Abidor's laptop and external drive, transmitted the contents of both devices to other agencies, and retained copies as well. Compl. ¶¶ 52-54.

Abidor claims that he now "self-censors" the information he stores on his computer—including the notes he might otherwise take in connection with his academic research—and warns those he interviews that his notes and any documents they provide to him might be viewed by border officials. Compl. ¶ 62. This has "change[d] the way he conducts research" and caused him to fear that interviewees will be less candid and share less information and fewer documents with him than they would have otherwise. Compl. ¶ 63.

### *C. The Association Plaintiffs' Allegations*

The NACDL alleges that many of its members—criminal defense attorneys resident throughout the country—routinely travel abroad for professional purposes and bring with them electronic devices containing personal, confidential, or privileged information. Compl. ¶¶ 69, 75–76. It contends that the ICE and CBP policies interfere with its members' ability to represent

clients because they must "take seriously the risk that the content of their electronic devices could be reviewed, copied, and detained." Compl. ¶ 77. This creates an ethical dilemma because NACDL's members have a duty to safeguard privileged and confidential information, which could be revealed to the federal government (a common litigation adversary for criminal defense attorneys) if their electronic documents are searched at the border. Compl. ¶ 79. NACDL alleges at least one of its member-attorneys was subject to a stop at the border. Compl. ¶¶ 85-95. The complaint alleges that her computer was taken "out of sight for more than 30 minutes, presumably to complete an electronic search." Compl. ¶ 95. The NACDL member "did not witness the CBP officer's search," and the laptop was returned after the 30 minute period. Compl. ¶ 95.[2]

The NPPA is a group of photojournalists who reside throughout the country and abroad and which promotes "freedom of the press in all its forms, especially as that freedom relates to photojournalism." Compl. ¶¶ 99-101. It alleges that its members routinely travel abroad and report on stories that are of interest to the United States government, which raises the specter of the targeted search and detention of their electronic materials without suspicion. In particular, they communicate with sources who request guarantees of anonymity that they may no longer be able to offer if their electronic devices are subject to search. Compl. ¶¶ 113-14. One photojournalist who was riding his motorcycle was allegedly stopped at the Canadian border. Compl. ¶¶ 122-27. "He had been in Canada to, among other things, take photographs for a piece on lighthouses and to take photos of national parks." Compl. ¶ 122. The complaint alleges that a CBP agent turned on the individual's computer, "and peruse[d] the contents of [the] laptop for

[2] The suggestion that the computer was "presumably" subject to a complete electronic search during the 30 minute period it was out of her presence is purely speculative. Indeed, such a search would have violated the CBP directive that absent specified exigent circumstances, such searches must be conducted in the presence of the individual whose information is being examined. CBP Directive § 5.1.4; *see also* ICE Directive § 8.1(2). I discuss this issue more fully in footnote 4.

approximately 15 minutes." Compl. ¶ 125. "[T]he [laptop's] password protection was not engaged because the laptop was in hibernate mode." Compl. ¶ 125. The CBP officer returned the laptop immediately after the alleged search. Compl. ¶ 125.

**DISCUSSION**

Before proceeding to a discussion of the issues of standing and the merits of the challenge to the CBP and ICE directives, it is important to define terms that are used to describe the challenged searches at issue here. One is a "quick look" and the other is a "comprehensive forensic examination." *See United States v. Cotterman*, 709 F.3d 952, 956, 960 (9th Cir. 2013). A quick look entails only a cursory search that an officer may perform manually. It involves opening the computer and viewing the computer's contents as any lay person might be capable of doing simply by clicking through various folders. *See, e.g.*, *Cotterman*, 709 F.3d at 960 (9th Cir. 2013) (during initial search of electronic devices, the officer simply "turned on the devices and opened and viewed image files"); *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008) (individual searched explained that "the CBP officers simply 'had me boot [the laptop] up, and looked at what I had inside'"). A forensic search, on the other hand, involves an exhaustive search of a computer's entire hard drive. "[F]orensic [search] software [] often must run for several hours to examine copies of the laptop hard drive[]." *Id.* at 958. Moreover, a forensic search enables officers to search a hard drive's unallocated space, which is the "space on a hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software. Such space is available to be written over to store new information." *Id.* at 958 n.4 (quoting *United States v. Flyer*, 633 F.3d 911, 918 (9th Cir. 2011)). The complaint challenges both kinds of searches.

### *A. Standing*

Plaintiffs bear the burden of establishing their standing to pursue the relief they seek. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). The "irreducible constitutional minimum" of standing requires a plaintiff to show that it has suffered a concrete and particularized injury in fact which is actual or imminent, not "conjectural or hypothetical," that there is a causal connection between the injury and the defendant's conduct, and that the injury will likely be redressed by a favorable decision. *Id.* at 560. The law of standing is built on separation-of-powers principles and, as such, the standing inquiry is "especially rigorous when reaching the merits of the dispute would force [the court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." *Raines v. Byrd*, 521 U.S. 811, 819-20 (1997).

A "threatened injury must be *certainly impending* to constitute injury in fact, and [] [a]llegations of *possible* future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1147 (2013) (second alteration in original) (internal quotation marks omitted). While *Clapper* acknowledges that in some instances standing has been found based on a "substantial risk" that the alleged harm will occur, *id.* at 1150 n.5, the plaintiffs cannot prevail under either because there is not a substantial risk that their electronic devices will be subject to a search or seizure without reasonable suspicion.[3] Moreover, whenever an association asserts standing solely as the representative of its members it "must allege that its members, or any one of them, are suffering immediate or threatened injury as a result of the challenged action of the sort that would make out a justiciable case had the members themselves brought suit." *Warth v Seldin*, 422 U.S. 490, 511 (1975).

[3] A more relaxed standard may be appropriate where the challenges to the enforcement against a plaintiff of a traditional punitive statute, whether civil or criminal, because of the presumption that the Executive Branch will enforce such laws. *See Hedges v. Obama*, 724 F.3d 170, 201 (2d Cir. 2013).

Relying on records released by the CBP through the Freedom of Information Act (FOIA), the complaint alleges that 6,500 people, less than 3,000 of whom were U.S. citizens, had their electronic devices subjected to search at the U.S. border between October 1, 2008 and June 2, 2010. Compl. ¶¶ 1, 20. The complaint goes on to allege that, over the seven month period between October 28, 2008 and June 9, 2009, "CBP detained over 220 electronic devices carried by international travelers." Compl. ¶ 20. This comes to a fraction less than one a day. The complaint, however, does not provide the information necessary to place these numbers in context. Nevertheless, such information is readily available.

Statistics compiled and published by the CBP in 2006 indicate that "[o]n a typical day, more than 1.1 million passengers and pedestrians . . . are processed at the nation's borders." *Securing America's Borders at Ports of Entry*, U.S. Customs and Border Protection, 2 (Sept. 2006), https://www.hsdl.org/?view&did=469950.[4] Using that figure, fewer than one in a million electronic devices were detained by the CBP. Stated another way, there is less than a one in a million chance that a computer carried by an inbound international traveler will be detained. Even in the case of a quick look and search of a computer, in which CBP officers simply have a traveler boot the laptop up, and look at what is inside, *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008), as opposed to a more comprehensive forensic search that would presumably occur if a computer were detained, the number of U.S. citizens subject to such a

[4] A judge can take judicial notice, on his own, of a fact that "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b), (c). The Court of Appeals for the Ninth Circuit appears to have done just that in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013). Indeed, the opening line in its opinion begins with the observation that "[e]very day more than a million people cross American borders with Mexico and Canada to functional borders at airports such as Los Angeles (LAX), Honolulu (HNL), New York (JFK, LGA), and Chicago (ORD, MDW)." *Id.* at 956. Moreover, the defendants have submitted a declaration from the Director of the Program Analysis and Measures Branch within the Policy, Program Analysis and Evaluation Division of the Office of Field Operations of the CBP, in which he declares that according to CBP systems 590 million inbound travelers crossed the border between October 1, 2008 and June 2, 2010. Riley Decl. ¶¶ 1, 4. The plaintiffs do not dispute this figure. Instead, they argue that "[m]atters outside of the pleadings may not be considered on a motion to dismiss under Rule 12(b)(6)." Pls.' Br. 3 n.1. Nevertheless, matters outside the pleadings, of which judicial notice may be taken, may be considered. 5C Charles Alan Wright, Arthur R. Miller & Mary Kay Kane, *Federal Practice and Procedure*, § 1367 (3d ed. 1998); *see also Roberts v. Babkiewicz*, 582 F.3d 418, 419 (2d Cir. 2009).

search comes to approximately 4.9 per day, or less than a five in a million chance that their computer will be subject to any kind of search. Even if both U.S. citizens and aliens are counted, there is about a 10 in a million chance that such a search will take place. *See United States v. Ickes*, 393 F.3d 501, 506-07 (4th Cir. 2005) (rejecting as "far-fetched" the suggestion that "any person carrying a laptop computer . . . on an international flight would be subject to a search of the files on the computer hard drive[,]" because "[c]ustoms agents have neither the time nor the resources to search the contents of every computer").

Care must be taken, however, not to conflate the number of searches at the border with the number of those searches that were undertaken without reasonable suspicion. The figures that the complaint cites overstate the odds of a suspicionless search, which plaintiffs allege violates the Constitution, because there is an even more remote chance that such a search would take place without suspicion. *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), a case upon which the plaintiffs rely, is instructive. The defendant there moved to suppress evidence that was obtained as a result of a forensic examination of his computer after an "initial search at the border [of his computer] turned up no incriminating material." *Id.* at 956. "Only after Cotterman's laptop was shipped almost 170 miles way and subjected to a comprehensive forensic examination" was incriminating evidence discovered. *Id.* The Ninth Circuit held that "the legitimacy of the initial search of Cotterman's electronic devices at the border is not in doubt," because the searching officer merely "turned on the devices and opened and viewed image files while the Cottermans waited to enter the country." *Id.* at 960.

Significantly, while the Ninth Circuit held that reasonable suspicion for the more comprehensive forensic examination was required, it acknowledged that the "government—for now—does not have the time or resources to seize and search the millions of devices that accompany the millions of travelers who cross our borders." *Id.* at 966. Even though the

regulations authorize such searches to take place without reasonable suspicion, the Ninth Circuit observed that "as a matter of commonsense and resources, it is only when reasonable suspicion is aroused that such searches will take place." *Cotterman*, 709 F.3d at 967 n.14; *see also United v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005) ("As a practical matter, computer searches are most likely to occur where—as here—the traveler's conduct or the presence of other items in his possession suggest the need to search further."). Indeed, in *Cotterman*, the Ninth Circuit held that the challenged searched was based on reasonable suspicion. *Id.* at 968-70. So too is the search of the individual plaintiff in this case, Pascal Abidor.

The Ninth Circuit's apparent concern was not with an ongoing practice of suspicionless comprehensive forensic computer searches of the kind it held "intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border." *Id.* at 966. Rather, although it acknowledged that "for now" such searches were beyond the government's resources, it was "the potential unfettered dragnet effect that [was] troublesome." *Id.* While the procedural posture of the *Cotterman* case—an appeal from an order granting the defendant's motion to suppress—provided an occasion for the Ninth Circuit to address the threshold issue whether reasonable suspicion was required for the search that took place in that case, the procedural posture of the present case makes such consideration inappropriate.

An action for declaratory judgment does not provide an occasion for addressing a claim of alleged injury based on speculation as to conduct which may or may not occur at some unspecified future date. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992); *Diamond v. Charles*, 476 U.S. 54, 66 (1986) (rejecting standing based on "unadorned speculation"); *City of Los Angeles v. Lyons*, 461 U.S. 95, 105, 111 (1983) (denying standing to an individual seeking to challenge police chokehold because it was only speculative that the plaintiff would be subjected to chokehold); *O'Shea v. Littleton*, 414 U.S. 488, 497 (1974) (denying standing to

residents who sought injunctive relief against judges who allegedly engaged in a pattern and practice of discriminatory practices on the ground that the threat to plaintiffs from this discrimination was only "speculation and conjecture").

In *Baur v. Veneman*, 352 F.3d 625 (2d Cir. 2003), upon which plaintiffs rely, a divided three judge panel addressed the "narrow question" of whether "an increased risk of contracting a food-borne illness from the consumption of downed livestock constitutes a cognizable injury-in-fact." *Id.* at 631. While that case acknowledged that "the 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," it did "not decide as a matter of law whether enhanced risk generally qualifies as sufficient injury to confer standing." *Id.* at 633-34. It held that "[i]n the specific context of food and drug safety suits," like in environmental cases, such injuries are cognizable for standing purposes. *Id.* at 634. This analysis, however, "has only been applied in a narrow range of cases," where "an agency's failure to conform to a statutory mandate has resulted in the plaintiff's exposure to a greater risk of an either difficult or impossible to remedy injury that the statute explicitly sought to prevent, and then, only in the context of exposure to environmental conditions or harmful products." *Nat. Council of La Raza v. Gonzales*, 468 F. Supp. 2d 429, 440 (E.D.N.Y. 2007).

*Baur* appears to mark a narrow exception to the rule that probabilistic injury does not provide a basis for Article III standing. As Judge Livingston has observed, "[p]robabilistic injury" of the kind on which *Baur* relied, has "never been recognized by the Supreme Court or this Circuit as sufficient as a general matter to constitute injury in fact for the purposes of Article III standing, and for good reason—as the D.C. Circuit has noted, were all purely speculative increased risks deemed injurious, the entire requirement of actual or imminent injury would be rendered moot, because all hypothesized, non-imminent injuries could be dressed up as increased

risk of future injury." *Amnesty Int'l USA v. Clapper*, 667 F.3d 163, 198 (2d Cir. 2011) (Livington, J, dissenting from denial of reh'g en banc) (internal quotation marks omitted). Such an approach she observed, "would threaten grossly to distend the Judicial Branch's proper role of deciding actual cases or controversies, rendering almost any governmental action or inaction at least potentially subject to judicial review so long as a court was willing to deem it "reasonably likely" that a plaintiff might one day be affected as a result." *Id.*[5]

Moreover, even assuming the allegations in the complaint established standing, closely related principles of declaratory judgment law warrant dismissal. Specifically, "[a] declaratory judgment, like other forms of equitable relief, should be granted only as a matter of judicial discretion, exercised in the public interest. It is always the duty of a court of equity to strike a proper balance between the needs of the plaintiff and the consequences of giving the desired relief." *Eccles v. Peoples Bank of Lakewood Vill.*, 333 U.S. 426, 431 (1948). Thus, "[e]specially where governmental action is involved, courts should not intervene unless the need for equitable relief is clear, not remote or speculative." *Id.*; *see also* 10B Charles Alan Wright, Arthur R. Miller & Mary Kay Kane, *Federal Practice and Procedure*, § 2762 (3d ed. 1998) ("The Supreme Court has frequently, although not invariably, indicated a marked reluctance to have important issues of public law resolved by declaratory judgments."). Such reluctance is particularly warranted as to the association plaintiffs because the special protections afforded to attorneys and journalists makes it impossible to determine whether, or to what extent, the directives on their face will actually result in any search, much less one without reasonable suspicion.

Significantly, in the context of the present case, delaying a decision provides an opportunity for Congress and the Executive Branch to respond to any abuses that should develop

[5] The petition for rehearing in *Amnesty Int'l USA v. Clapper* was denied by an equally divided vote. *Amnesty Int'l USA v. Clapper*, 667 F.3d at 163-64 (2d Cir. 2011). Judge Livingston's opinion was joined by then-Chief Judge Jacobs, and Judges Cabranes, Raggi, and Wesley. *Id.* at 164. The Supreme Court granted certiorari, 132 S.Ct. 2531 (2012), and reversed the panel opinion in *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138 (2013).

as a consequence of the operation of the current CBP and ICE directives—directives which themselves seek to regulate and circumscribe the conduct of searches of electronic devices. *See* Yule Kim, Cong. Research Serv. RL34404, *Border Searches of Laptop Computers and Other Electronic Storage Devices*, 13-14 (2009) (describing recent legislative proposals to limit border searches of electronic devices). Indeed, a careful reading of the CBP and ICE directives indicates that these agencies are sensitive to the privacy and confidentiality issues posed by border searches of electronic devices. They constitute efforts to cabin the nature and extent of such searches, and they contain significant precautionary measures to be taken with respect to the handling of privileged and other sensitive materials that are described earlier. CBP Directive § 5.2; ICE Directive § 8.6; *see supra* discussion at 6-7.

Thus, upon the assertion by an individual that "certain information is protected by attorney-client or attorney work product privilege," or if it appears that the electronic device contains such material, both the CBP and ICE directives preclude any search of an electronic device without seeking advice from the agency's Chief Counsel, who must make a record of such consultation in the system of records, and coordinate with the U.S. Attorney's Office as appropriate. CBP Directive § 5.2.1; *see also* ICE Directive § 8.6(2)(b). Indeed, I read these particular directives as containing a significant threshold requirement. Specifically, even before consulting legal counsel within the agency, a CBP or ICE officer must suspect that such material constitutes evidence of a crime or otherwise pertains to a determination within the jurisdiction of the CBP or ICE. *Id.* Moreover, reasonable suspicion and probable cause are required for certain conduct to be undertaken, other than the search itself. *See, e.g.*, CBP Directive § 5.3.2.3, 5.4.1.1; ICE Directive §§ 8.4(2)(b), 8.5(1)(a). Significantly, some of the reported cases indicate that search warrants were obtained for comprehensive forensic searches, even though not required by

the directives. *See, e.g.*, *United States v. Stewart*, 729 F.3d 517, 521 (6th Cir. 2013); *United States v. Arnold*, 533 F.3d 1003, 1005 (9th Cir. 2008).

In sum, declaratory relief is not appropriate because is it unlikely that a member of the association plaintiffs will have his electronic device searched at the border, and it is far less likely that a comprehensive forensic search would occur without reasonable suspicion. This is particularly true with respect to electronic devices of lawyers and journalists, among others, who have been singled out for special protection. *See* CBP Directive § 5.2; ICE Directive § 8.6. Indeed, Pascal Abidor, the only individual plaintiff in the case, who claims to have had his computer subject to a forensic search upon his entry into the United States from Canada, by his own admission travels frequently between the United States and Canada, was stopped two more times at the border. His was not computer subject to a search of any kind on either occasion. Compl. ¶ 58; Abidor Decl. ¶ 7; Allen Decl ¶ 11.[6]

Nor is there any merit to Abidor's claim that he has standing "for the additional reason that he seeks expungement of information he believes DHS may have retained from his electronic devices. Pls.' Br 18. He argues this is an ongoing injury, and that "the Second Circuit has recognized" a demand for expungement provides a basis for standing. Pls.' Br. 18. The

[6] The circumstances surrounding the last search, which took place December 22, 2010, are not spelled out in the complaint. Instead, they are described in post-complaint declarations by Abidor and Charles Allen, the Supervisory CBP Officer at the Port of Champlain, New York, where the events occurred. Abidor Decl.; Allen Decl. Abidor alleges only that "[a]n agent took two cell phones out of sight." Abidor Decl. ¶ 7. In a reply declaration, Officer Allen acknowledges that the two cell phones were taken pursuant to general "CBP practice with respect to secondary inspection," that "all electronic devices, including cell phones, are requested of the individuals being inspected at the start of the inspection so that the devices cannot be used during the inspection process." Allen Decl. ¶¶ 7-9. Allen goes on to say "[a]t no time . . . were the cell phones searched, nor was the information contained in them examined or copied in any manner." Allen Decl. ¶ 11. The only inconsistency between the two affidavits is Allen's assertion that "the cell phones were simply placed on the secondary work station out of Pascal's and [his father's] reach but within their plain view." Allen Decl. ¶ 11. This is consistent with the CBP directive that "[s]earches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit the individual to remain present." CBP Directive § 5.1.4; *see also* ICE Directive § 8.1(2). Passing over the propriety of the submission of these affidavits in the context of a motion to dismiss, and accepting Abidor's version of the events, it does not establish that any search occurred. Indeed, the fact that this incident is the only one that plaintiffs have chosen to document during the three years since they filed the complaint, only confirms that it is unlikely that any of the plaintiffs will have their electronic devices searched at the border.

problem with this argument is that under the regulations he is entitled to have the materials destroyed. CBP § Directive 5.3.2.4. Indeed, the Department of Justice attorney conceded at oral argument that the materials "would have been destroyed but for the fact that cases had been filed," and that they were being retained as potentially relevant to those cases. Hr'g Tr., 32:4-29 (June 8, 2011). Under these circumstances, the fact that Abidor seeks expungement does not provide a basis to challenge a regulation which provides him with that remedy. *See Cherry v. Postmaster Gen.*, 332 F. Supp. 785, 789 (S.D.N.Y. 1971), *aff'd* 460 F.2d 1063 (2d Cir. 1972).

Abidor could have established standing in this case by adding a cause of action for damages based on his claim that he was subject to an unreasonable search. Such a cause of action would have provided the occasion for a trial or a motion for summary judgment that would have fully developed the record with respect to both the initial quick look search and subsequent forensic search. No such action is alleged. Instead, it appears that Abidor was chosen to participate as a co-plaintiff because, unlike any member of the association plaintiffs, his computer was subject to a search pursuant to the directives that are challenged here. Nevertheless, as the Supreme Court held in *City of Los Angeles v. Lyons*, even given past harm, "[a]bsent a sufficient likelihood that [the plaintiff] will again be wronged in a similar way, [he] is no more entitled to an injunction than any other citizen." 461 U.S. at 111.

Plaintiffs try to bolster their claim for standing in several ways. The NACDL alleges that its members routinely travel abroad to "collaborate with foreign colleagues and/or as part of their representation of their clients." Pls.' Br. 8. They almost always travel with electronic devices because those devices "are necessary to take notes, record interviews, perform legal research, draft legal documents, retrieve case files, and communicate." Pls.' Br. 8. The NACDL goes on to allege that because its "members have an ethical duty to safeguard attorney-client and other privileged information, they must spend time and money to mitigate the harm that future

searches will cause." Pls.' Br. 8 (internal citation omitted). Similarly, the NPPA argue that the challenged policies "undermine NPPA members' ability to guarantee confidentiality to the sources they communicate with abroad." Pls.' Br. 9. Consequently, "[t]he risk [their] sources' identities will be revealed to border agents . . . will lead some sources who otherwise would have shared information or been recorded, photographed, or videotaped to decline to do so." Pls.' Br. 9.

The individual plaintiff, Pascal Abidor, alleges that he plans to undertake additional travel to conduct research in foreign countries, including Syria and Lebanon, Pls.' Br. 7, apparently unconcerned about the searches to which his computer may be subject in those countries. He argues that, "at the expense of his educational goals," he has expended time and money to minimize future searches at the United States border. Pls.' Br. 7. Thus, "[h]e 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." Pls.' Br. 7-8. Moreover, he asserts that [h]e now avoids taking notes for his research and gathering materials of the type that might be misconstrued by border officials and warns research subjects that he cannot guarantee them confidentiality." Pls.' Br. at 8.

Because plaintiffs do not face a threat of certainly impending suspicionless border searches of their electronic devices, they cannot establish standing based on the measures they have undertaken to preserve confidentiality of the sensitive information they claim would be compromised as a result of the searches that the challenged directives authorize. *See Clapper*, 133 S.Ct. at 1152 n.7. Indeed, laptops have only come into widespread use in the twenty-first century. Prior to that time, lawyers, photographers, and scholars managed to travel overseas and consult with clients, take photographs, and conduct scholarly research. No one ever suggested the possibility of a border search had a chilling effect on his or her First Amendment rights.

While it is true that laptops may make overseas work more convenient, the precautions plaintiffs may choose to take to "mitigate" the alleged harm associated with the remote possibility of a border search are simply among the many inconveniences associated with international travel. In this regard, plaintiffs are no different than the tens of millions of international travelers who cross the United States border.

More significantly, however, it is difficult to understand how a threshold requirement of reasonable suspicion significantly alleviates the alleged harm that plaintiffs fear. Reasonable suspicion is a minimal threshold standard for conducting a search. Indeed, in *Cotterman*, the Ninth Circuit reaffirmed an earlier holding that reasonable suspicion was not required for "a quick look and unobtrusive search of laptops." *Cotterman*, 709 F.3d at 960, 967. The quick look and search in the prior case was one in which CBP officers simply "had [traveler] boot [the laptop] up, and looked at what [he] had inside." *Arnold*, 533 F.3d at 1009. Moreover, such searches could result in "further, forensic examinations where their suspicions are aroused by what they find or by other factors. Reasonable suspicion leaves ample room for agents to draw on their expertise and experience to pick up on the subtle cures that criminal activity may be afoot." *Cotterman*, 709 F.3d at 967.

Plaintiffs must be drinking the Kool-Aid if they think that a reasonable suspicion threshold of this kind will enable them to "guarantee" confidentiality to their sources, Pls.' Br. 8-9, or to protect privileged information, Pls.' Br. 8. Nor is this the only consideration that prevents them from guaranteeing confidentiality. The United States border is not the only border that must be crossed by those engaging in international travel. "Carrying an electronic device outside the United States almost always entails carrying it into another country, making it subject to search under that country's laws." *Cotterman*, 709 F.3d at 977 n.8 (Callahan, J., dissenting). Surely, Pascal Abidor cannot be so naïve to expect that when he crosses the Syrian or Lebanese

border that the contents of his computer will be immune from searches and seizures at the whim of those who work for Bashar al-Assad or Hassan Nasrallah. Indeed, the New York Times recently reported on the saga of David Michael Miranda who was detained for nine hours by British authorities "while on a stop in London's Heathrow airport during a trip from Germany to Brazil." Charlie Savage & Michael Schwartz, *Britain Detains the Partner of a Reporter Tied to Leaks*, The New York Times, A4 (Aug. 19, 2013). Miranda was carrying documents intended to be passed to a British journalist. *Id.* Those documents were stored on encrypted thumb drives—a data storage device—and were seized. *Id.* The stop and search were undertaken pursuant to the United Kingdom Terror Law Schedule 7, which authorizes such searches without reasonable suspicion. U.K. Terror Law Schedule 7 § 8.

This is enough to suggest that it would be foolish, if not irresponsible, for plaintiffs to store truly private or confidential information on electronic devices that are carried and used overseas. There is yet another reason—the risk associated with the loss of laptop computers. A recent comprehensive study of airports and business travelers, sponsored by Dell Inc., reported that "[b]usiness travelers in the U.S., Europe and [the] United Arab Emirates lose or misplace more than 16,000 laptops per week." *Airport Insecurity: The Case of the Lost & Missing Laptops*, Ponemon Institute LLC, 3 (July 29, 2008), http://www.dell.com/downloads/global/services/dell_lost_laptop_study_emea.pdf. These laptops were either lost or stolen. *Id.* One of the many suggestions that the Dell study makes to travelers is to "[t]hink twice about the information you carry on your laptop." *Id.* at 8. And it concludes with the commonsense query: "Is it really necessary to have so much information accessible to you on your computer?" *Id.*

### *B. The Merits*

While I do not believe that the plaintiffs have standing, I discuss the merits of their claims in order to complete the record and avoid the possibility of an unnecessary remand in the event that the Court of Appeals shall disagree. I agree with the Ninth Circuit that reasonable suspicion is not required to conduct a cursory manual search of an electronic device at the border. *Cotterman*, 709 F.3d at 960. I also agree with the Ninth Circuit that the transport of an electronic device away from the border to perform a forensic search is not a dispositive fact, and "the extended border search doctrine does not fit th[at] search." *Id.* at 962. Finally, I agree with the reasons stated in the thoughtful and considered opinion of Judge Wilkinson in *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), which the Ninth Circuit adopted in *United States v. Arnold*, 533 F.3d 1003, 1010 (9th Cir. 2008) (O'Scannlain, J.), for refusing to carve out a First Amendment exception to the border search doctrine.[7] I focus here on the issue of whether a comprehensive forensic search can only be undertaken based on reasonable suspicion.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. Const. amend. IV. Whether a search or seizure is unreasonable "depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself. The permissibility of a particular law enforcement practice is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) (internal quotation marks and citations omitted). "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States*

[7] While the en banc opinion in *Cotterman* limited the scope of the holding in *Arnold* regarding the restrictions the Fourth Amendment places on comprehensive forensic searches of electronic devices at the border, *Cotterman* did not upset the First Amendment holding in *Arnold*.

*v. Flores-Montano*, 541 U.S. 149, 152–53 (2004). Accordingly, "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior. Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant, and first-class mail may be opened without a warrant on less than probable cause." *Montoya de Hernandez*, 473 U.S. at 538 (internal citations omitted).

> Border searches . . . from before the adoption of the Fourth Amendment, have been considered to be "reasonable" by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless "reasonable" has a history as old as the Fourth Amendment itself.

*United States v. Ramsey*, 431 U.S. 606, 619 (1977). "Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in and his belongings as effects which may be lawfully brought in." *Carroll v. United States*, 267 U.S. 132, 154 (1925); *see also United States v. Singh*, 415 F.3d 288, 293 (2d Cir. 2005) (same).

Professor LaFave observes that, "[a]lthough it has sometimes been said that mere entry into the United States gives rise to probable cause for a search, this is hardly the case, for certainly the great majority of persons entering the country are not engaged in the smuggling of contraband." 5 Wayne LaFave, *Search and Seizure: A Treatise of the Fourth Amendment*) § 10.5(a) (4th Ed. 2011-12). Instead, he continues, "[t]he point is . . . that probable cause is not required for such a search." *Id.* Similarly "[i]t is also sometimes said in the cases that mere suspicion is needed to conduct a routine border search, which would seem to require at least some knowledge identifying an individual as a suspect, with that information being operated on

by experienced customs agents." *Id.* (internal quotation marks omitted). Nevertheless, "this is likewise not the case, and it is more accurate to say that even mere suspicion is not required." *Id.* (internal quotation marks omitted). Indeed, "[a]ny person or thing coming into the United States is subject to search by that fact alone, whether or not there be any suspicion of illegality directed to the particular person or thing to be searched." *Id.* (internal quotation marks omitted).[8]

The border search doctrine is an example of what is known as an administrative or special needs exception to traditional threshold requirements of probable cause and reasonable suspicion. *See, e.g.*, *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 679 (1989); *Skinner v. Ry. Lab. Exec. Ass'n*, 489 U.S. 602, 633-34 (1989). The leading case outlining the considerations underlying administrative search exceptions is *Camara v. Municipal Court*, 387 U.S. 523 (1967). There, the Supreme Court upheld another kind of administrative search, the health and safety exception of buildings, "upon reasoning which is equally applicable to the border search." LaFave, § 10.5(a). In so doing, it concluded that:

> no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails. But we think that a number of persuasive factors combine to support the reasonableness of area code-enforcement inspections. First, such programs have a long history of judicial and public acceptance. Second, the public interest demands that all dangerous conditions be prevented or abated, yet it is doubtful that any other canvassing technique would achieve acceptable results. Many such conditions-faulty wiring is an obvious example-are not observable from outside the building and indeed may not be apparent to the inexpert occupant himself. Finally, because the inspections are neither personal in nature nor aimed at the discovery of evidence of crime, they involve a relatively limited invasion of the urban citizen's privacy.

[8] The only recognized exception to this broad holding, which has been carved out by the Courts of Appeals, relates to strip and body cavity searches. *See United States v. Asbury*, 586 F.2d 973 (2d Cir. 1978); *see also* LaFave § 10.5(b) (collecting cases). The Supreme Court, however, has left open the issue of "what level of suspicion, if any is required for nonroutine border searches, such as strip, body cavity, or involuntary x-ray searches." *Montoya de Hernandez*, 473 U.S. at 546 n.4. Nevertheless, the Supreme Court has made it clear that the need for particularized reasonable suspicion does not apply to highly intrusive searches of property at the border. *Flores-Montano*, 541 U.S. at 152.

*Camara*, 387 U.S. at 536-37.

Border searches, likewise, "have a long history of judicial and public acceptance." *Id.* at 537. Indeed, "border searches . . . from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside." *Ramsey*, 431 U.S. at 619. Such searches were first authorized by the same Congress which proposed the Bill of Rights. *Flores-Montano*, 541 U.S. at 153. Moreover, as Professor LaFave observes, "[c]entral to the *Camara* holding was the fact that the administrative search there at issue was directed at a problem as to which there was a strong public interest in effective preventive measures and which could not be dealt with effectively if the authorities were required to have probable cause [or reasonable suspicion] on a case-by-case basis." LaFave, § 10.5(a). This is equally true of the searches laptop computers and other similar electronic devices at the border.

> Laptop searches have proven essential to detecting people and materials that should be blocked from entering the United States. Officers have discovered video clips of improvised explosive devices being detonated, a martyrdom video and other violent jihadist materials. In addition, these searches have uncovered scores of instances of child pornography, including a home movie of children being sexually assaulted.

Michael Chertoff, *Searches Are Legal, Essential*, USA Today, July 16, 2008, at A10.

As in *Camara*, "it is doubtful that any other canvassing technique would achieve acceptable results." *Camara,* 387 U.S. at 537. "[C]ustoms officials do not usually have specific knowledge of a person or goods before their inspection. In the absence, therefore, of a broad power of search at the border, officials would commonly have to rely on the cooperation of those they question." Judith B. Ittig, *The Rites of Passage: Border Searches and the Fourth Amendment*, 40 Tenn L. Rev. 329, 331 (1973).

The final consideration in *Camera* was that the inspection at issue in that case were not aimed at the discovery of evidence, and involved "a relatively limited invasion of . . . privacy." A comprehensive forensic search of a computer, whether a desktop or a laptop, involves a significant invasion of privacy. *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013); *see also United States v. Mitchell*, 565 F.3d 1347, 1352 (11th Cir. 2009). The invasion of privacy occasioned by such a border search, however, like the search of luggage, briefcases, and even clothing worn by a person entering the United States, is mitigated by other factors that are not present in a purely domestic context. As Professor LaFave observes, because "the individual crossing a border is on notice that certain types of searches are likely to be made, his privacy is less invaded by those searches." LaFave, § 10.5(a). Thus, "[t]he individual traveler determines the time and place of the search by his own actions, and he thus has ample opportunity to diminish the impact of that search by limiting the nature and character of the effects which he brings with him." *Id.*[9] Indeed, because of the large number of laptop computers (close to a million per year) that are lost by travelers—numbers that far exceed the comparative handful of laptops that are searched at the border—the sensible advice to all travelers is to "[t]hink twice about the information you carry on your laptop," and to ask themselves: "Is it really necessary to have so much information accessible to you on your computer?" *Airport Insecurity* at 8.

The Second Circuit has not addressed the issue of border searches of electronic devices. But in *United States v. Irving*, No. S3-03-0633, 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003), Judge Kaplan held that laptop computers are analogous to other closed containers, which may be inspected without reasonable suspicion or probable cause in a routine border search.

[9] "The element of choice is crucial. The fact that border searches occur at fixed times and checkpoints makes them inherently less intrusive; a person 'with advance notice of the location of a permanent checkpoint has an opportunity to avoid the search entirely, or at least to prepare for, and limit, the intrusion on her privacy.'" *Cotterman*, 709 F.3d at 978 (Callahan, J., dissenting) (citing *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 463 (1990) (Stevens, J., dissenting).

There, customs agents conducted a search of undeveloped film in a disposable camera and two 3.5 inch computer diskettes. *Id.* at *2. In rejecting that such a search required reasonable suspicion, Judge Kaplan observed:

> Inspection of the contents of closed containers comes within the scope of a routine border search and is permissible even in the absence of reasonable suspicion or probable cause. Indeed, the opening of luggage, itself a closed container, is the paradigmatic routine border search. Hence, the agents were entitled to inspect the contents of the diskettes even absent reasonable suspicion. Indeed, any other decision effectively would allow individuals to render graphic contraband, such as child pornography, largely immune to border search simply by scanning images onto a computer disk before arriving at the border.

*Id.* at *5. Because the Second Circuit upheld the validity of the search on the ground that it was supported by reasonable suspicion, it did not reach the issue resolved by Judge Kaplan. *United States v. Irving*, 452 F.3d 110 (2d Cir. 2006).

Outside of this circuit, three Courts of Appeals have addressed the question. The Third and Fourth Circuits held that searches of electronic devices constitute routine border searches. *United States v. Linarez-Delgado*, 259 F. App'x 506, 508 (3d Cir. 2007) ("Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search."); *United States v. Ickes*, 393 F.3d at 506–07 (rejecting defendant's argument that "expressive materials"—such as defendant's computer and disks, which contained child pornography—are shielded by the First Amendment from routine border searches).

Nevertheless, the Ninth Circuit recently held that border searches of electronic devices may require reasonable suspicion in some circumstances. *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc). In that case the defendant was detained at the U.S.-Mexican border because of a positive hit on the Treasury Enforcement Communication System, which "indicated that [he] was a sex offender . . . and that he was potentially involved in child sex

tourism." *Id.* at 957. The defendant's two laptop computers and a digital camera were held for examination. *Id.* at 957–58. Officers discovered images of child pornography after a thorough forensic examination of the defendant's laptop. *Id.* at 958–59.

The Court of Appeals differentiated between what it referred to as a "forensic examination" and the "quick look" it had previously approved without a suspicion requirement in other cases. *Cotterman*, 709 F.3d at 960–61 (citing *Arnold*, 533 F.3d at 1009 (9th Cir. 2008)). The *Cotterman* Court relied on the question left open by the Supreme Court since *United States v. Ramsey*, 431 U.S. 606 (1972), of when a "'particularly offensive' search might fail the reasonableness test." *Cotterman*, 709 F.3d at 963 (citing *Ramsey*, 431 U.S. at 618 n.13). It went on to find that because of the volume and sensitivity of the material present on a modern laptop the "exhaustive forensic search of a copied laptop hard drive intrudes upon privacy and dignity interests to a far greater degree than a cursory search at the border." *Id.* at 966. Because of what it perceived as the deeply intrusive nature of the search, the Ninth Circuit held that "the forensic examination of [the defendant's] computer required a showing of reasonable suspicion." *Id.* at 968. Nevertheless, it ultimately concluded that there was reasonable suspicion to search the defendant's laptop and therefore reversed the district court's grant of the motion to suppress. *Id.* at 970.

As I have previously observed, the Ninth Circuit acknowledged that its opinion would not have any practical effect on current practices, because the extremely limited resources available to conduct comprehensive forensic searches necessarily limits such searches to situations where some level of suspicion is present. *Id.* at 967 n.14. I would agree with the Ninth Circuit that, if suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required. Now, however, "locking in a

particular standard for searches would have a dangerous, chilling effect as officer's often split-second assessments are second guessed." Chertoff, *Searches Are Legal, Essential*.[10]

This leaves one last point—Abidor's as applied challenge to the quick look and comprehensive forensic searches of his electronic devices. There was reasonable suspicion for those searches. "A reasonable suspicion inquiry simply considers, after taking into account all the facts of a particular case, 'whether the border official ha[d] a reasonable basis on which to conduct the search.'" *Irving*, 452 F.3d at 124 (quoting *United States v. Asbury*, 586 F.2d 973, 975–76 (2d Cir. 1978)). Reasonable suspicion is a relatively low standard and border officials are afforded deference due to their training and experience. *See Montoya de Hernandez*, 473 U.S. at 542. In *Asbury*, the Second Circuit identified a number of factors that have been deemed significant in evaluating whether law enforcement officers have a reasonable suspicion of possible criminal activity, including "[a]n itinerary suggestive of wrongdoing" and "[d]iscovery of incriminating matter during routine searches," *Asbury*, 586 F.2d at 977, both of which were present in this case.

In Abidor's case, CBP agents observed images of the rallies of designated terrorist groups (Hamas and Hezbollah) on the laptop computer of a traveler who had recently traveled to Lebanon. According to the State Department report in effect at the time of the search, "[Hamas] retains a cadre of leaders and facilitators that conducts diplomatic, fundraising, and arms-smuggling activities in Lebanon, Syria, and other states," and was "increasing its presence in the Palestinian refugee camps in Lebanon." *See* Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2008, Terrorist Organizations*, U.S. Dep't of State (April 30,

[10] The Directive also authorizes CBP agents to copy the information stored on electronic devices to facilitate inspection. *See, e.g.*, CBP Directive § 5.3.1; ICE Directive § 8.1(4)–(5). Plaintiffs argue that merely copying information stored on an electronic device, to permit the information to be inspected, constitutes a separate, invasive search. Pls.' Br. 26. On the assumption that it is permissible to perform a forensic search of an electronic device, transferring information to a different storage device for the same sort of inspection does not transform the search from routine to non-routine (i.e., highly-intrusive into the dignity and privacy interests of the person searched).

2009), http://www.state.gov/j/ct/rls/crt/2008/122449.htm. Hezbollah is based in Lebanon and "has strong influence in Lebanon's Shia community." *Id.* When Abidor was asked why he was interested in these images, "Abidor explained that his specific area of research for his Ph.D. degree is the modern history of Shiites in Lebanon," in which Hezbollah openly operates. Compl. ¶ 32. Even if this may have explained the pictures of Hezbollah, it did not explain why Abidor saved the pictures of Hamas, a terrorist organization not composed of Shiites and not based in Lebanon.

Moreover, although Abidor told officers he was living in Canada, he possessed both a U.S. and French passport, Compl. ¶¶ 26, 28, a circumstance which, while perhaps innocent in itself, in combination with other factors may have increased the level of suspicion, especially as the passport containing the visas from Lebanon and Jordan was not produced initially. *See United States v. Sokolow*, 490 U.S. 1, 9 (1989) (several factors which by themselves are "consistent with innocent travel" may, taken together, "amount to reasonable suspicion"). The agents certainly had reasonable suspicion supporting further inspection of Abidor's electronic devices.

**CONCLUSION**

The motion to dismiss is granted.

**SO ORDERED.**

Brooklyn, New York
December 31, 2013

Edward R. Korman
Edward R. Korman
Senior United States District Judge