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

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 r-

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

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 h.08 0 ..

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 injle2(jl)-5-icut 0 Tw 4.64 0 Td02 Tc 0.368 Tw 0.8.57 -211.48uhjltu

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

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

aequence of thBD10(e)-6(ope)4(r)3(a)4(t)-2(i)-2(scnof)3(t)-2(he)-6(c)4(ur)-7(r)3(e)4(nBD10(t)-2(C)-3(B)7(

awn

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]o20.87 0 Td (13(J)-6(e(

B.

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

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

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 are afforded deference due to their tr

[10] The Directive also authorizes CBP agents to copy the information stored on electronic devices to

1(4)–(5). Plaintiffs argue that merely to be inspected, constitutes a separate, orensic search of an electronic pection does not transform the acy interests of the person

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,