THE FUTURE OF THE FOURTH AMENDMENT IN A DIGITAL EVIDENCE CONTEXT: WHERE WOULD THE SUPREME COURT DRAW THE ELECTRONIC LINE AT THE INTERNATIONAL BORDER?

Patrick E. Corbett[*]

[*] Professor of Criminal Law & Criminal Procedure, Thomas M. Cooley Law School, Lansing, Michigan. The author thanks the National Center for Justice and the Rule of Law, and Professor Thomas Clancy, for inviting him to participate in the 2011 Fourth Amendment Symposium. The author also wishes to acknowledge the detailed, timely, and academic research of Cooley Law School librarian, Jamie Baker, law students, Katherine Montgomery and Shawn Solon, as well as the helpful reflections of law student Jason Taylor.

INTRODUCTION

In 1980, the United States Supreme Court stated that "[i]n terms that apply equally to seizures of property and to seizures of persons, the Fourth Amendment has drawn a *firm line at the entrance to the house*. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant."[1] In 2001, in ruling that law enforcement use of a thermal imager pointed at a home to gather information regarding heat within the home violated the Fourth Amendment, the Court revisited the "firm line": "That line, we think, must be not only firm but also bright—which requires clear specification of those methods of surveillance that require a warrant."[2]

The Court has certainly made clear that what goes on in the home is private and heavily protected by the Fourth Amendment. Are there other areas where one's expectation of privacy is so high that the Court should draw a similar line? What about the intimate details of one's personal life that can be stored on a laptop computer (or other electronic devices)? Should United States Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) agents be allowed to search these items at the international border without any individualized suspicion? If they seize them without any suspicion, how long can they hold them, and how extensively can they search them before they run afoul of the Fourth Amendment? If the United States Supreme Court is faced with these questions, how will it likely rule?

---

[1] Payton v. New York, 445 U.S. 573, 590 (1980) (emphasis added).

[2] Kyllo v. United States, 533 U.S. 27, 40 (2001).

In a day and age when everyone travels with electronic devices—such as cell phones, laptops, flash drives, and digital cameras—it should come as no surprise that these devices are subject to a search when entering the United States.[3] While some sort of individualized suspicion is typically necessary for a search of one's personal belongings to be constitutional under the Fourth Amendment, the border search has been a longstanding exception to that rule. As a general matter, the high government interest in national security has empowered the Court to allow most border searches to occur without any individualized suspicion. While the law on border searches seems rock solid, will the deeply personal and private nature of data stored on electronic devices empower a change in the law? Will the vastness of the storage capacity of these devices motivate the Court to re-examine Fourth Amendment principles at the international border?

Using a case involving an international border search of a laptop, this Article will explore the future of the Fourth Amendment in a digital evidence context. Section I will review *Abidor v. Napolitano*,[4] a case recently filed by the American Civil Liberties Union and other entities asserting that United States border patrol policies that allow full searches of electronic storage devices, like a laptop computer, without any individualized suspicion violate the Fourth Amendment.[5] Section II will summarize what other courts have ruled in similar contexts. Section III will briefly examine Supreme Court border search

---

[3] Growing up near Detroit's Ambassador Bridge, linking Detroit to Windsor, Ontario, this author is no stranger to crossing the border and being extensively questioned or searched at the border. In fact, the Ambassador Bridge is North America's busiest border crossing. Detroit Int'l Bridge Co. v. Fed. Highway Admin., No. 09-13805, 2010 U.S. Dist. LEXIS 13671, at *1 n.1 (E.D. Mich. Feb. 17, 2010).

[4] Complaint, Abidor v. Napolitano, No. CV10-4059 (E.D.N.Y. filed Sept. 7, 2010) [hereinafter Abidor Complaint]. While the future of the *Abidor* case is unclear, the facts of *Abidor* provide a great backdrop for examination of the Fourth Amendment in the context of electronic devices at the border. This Article will not explore the likelihood that the *Abidor* case, or a similar case, will be accepted by the U.S. Supreme Court for review. For purposes of this Article, the author requests the reader to assume that the Court is willing to review such a case—how would they rule?

[5] Individuals seeking redress for losses due to the international border seizure and search of their laptops are not limiting themselves to Fourth Amendment claims. *See, e.g.*, Kam-Almaz v. United States, 96 Fed. Cl. 84 (Fed. Cl. 2011) (Due to jurisdictional concerns, plaintiff unsuccessfully sought redress under a breach of contract theory and the "takings" clause of the Fifth Amendment.).

cases and other arguably applicable Supreme Court opinions. Section IV will consider an assortment of concepts in an attempt to examine how a future panel of the United States Supreme Court might rule if faced with the issues presented in *Abidor*. The Article will conclude with parting reflections on how a future panel of the Supreme Court might rule. Will the Court draw an electronic line similar to that "firm line" at the entrance to the home?

I. *ABIDOR V. NAPOLITANO* AND BORDER SEARCHES OF ELECTRONIC STORAGE DEVICES

On September 7, 2010, Pascal Abidor, a Ph.D. student in Islamic studies studying in Canada with dual U.S. and French citizenship, and other plaintiffs,[6] filed a complaint against Secretary of the Department of Homeland Security (DHS), Janet

---

[6] Pascal Abidor is joined in this lawsuit by the National Association of Criminal Defense Lawyers (NACDL) and the National Press Photographers Association (NPPA). This case study will primarily focus on the situation faced by Pascal Abidor.

Plaintiff NACDL is a non-profit organization of criminal defense lawyers with a particular interest on the impact modern national security policies have had on First, Fourth, Fifth, and Sixth Amendment rights. Abidor Complaint, *supra* note 4, at 16. According to the complaint, in the course of their work, many NACDL attorneys often travel abroad to represent their clients and bring along electronic devices to record their work product, which necessarily contain confidential client information protected by the attorney-client privilege. *Id.* at 16-24. In today's society, NACDL asserts it is nearly impossible for attorneys to perform their duties without the aid of electronic devices, such as laptops. *Id.* According to the complaint, at least one member of the NACDL, criminal defense attorney Lisa M. Wayne, had her laptop searched during a forty-five minute long detention upon entering the United States after a business trip to Mexico. *Id.* 21-22.

Plaintiff NPPA is composed of 7000 professional and freelance photojournalists who advocate the free dissemination of information and images around the world. *Id.* at 25. According to the complaint, many of their members frequently travel the world to cover news stories including foreign conflicts of interest to the United States government. *Id.* at 26-27. They record their findings via text, images, video, audio recordings, and the like on various forms of electronic devices such as laptops. They assert that the Department of Homeland Security regulations put their First Amendment-protected and confidential material at risk of exposure when crossing the border, and detention of their devices makes it impossible for them to meet deadlines. *Id.* at 31-33. According to the complaint, NPPA member Duane Kerzic, a freelance photographer, had his laptop searched during his trip back from Canada to take photographs of lighthouses and national parks. *Id.*

Napolitano, attacking two new CBP and ICE policies of DHS[7] issued in August 2009.[8] In the complaint, Abidor asserted that the United States border patrol policies that allow full searches of electronic storage devices, like a laptop computer, without any individualized suspicion, violate the violate the First and Fourth Amendments.[9]

In May 2010, Pascal Abidor was traveling via Amtrak train from Montreal, Canada to New York City.[10] Abidor had recently traveled to Jordan and Lebanon for academic purposes.[11] When the train arrived at the CBP point at the Canada–United States border, routine questioning of Abidor led the CBP officer to request that Abidor sign into his password-protected laptop for an additional search of the electronic data it contained.[12] The CBP officer perused some of his personal data (such as photos and saved chat conversation with his girlfriend) and some information and images downloaded for research purposes, including images of Hamas and Hezbollah rallies.[13] After writing down the password for the officer, Abidor was frisked and then transferred to Service Port-Champlain where he was detained in a small cinderblock cell and questioned for several hours.[14] After he was released, officers

---

[7] U.S. CUSTOMS AND BORDER PROTECTION, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION, CBP DIRECTIVE NO. 3340-049 (2009) [hereinafter 2009 CBP DIRECTIVE], *available at* http://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf; U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, BORDER SEARCHES OF ELECTRONIC DEVICES, ICE DIRECTIVE NO. 97-6.1 (2009) [hereinafter 2009 ICE DIRECTIVE], *available at* http://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf. CBP and ICE are two components of the United States Department of Homeland Security. *See* DEPARTMENT OF HOMELAND SECURITY, http://www.dhs.gov/index.shtm (last visited Jan. 25, 2012).

[8] *See* Abidor Complaint, *supra* note 4, at 4.

[9] *See id.* at 25-33. At the time of this writing, the *Abidor* complaint was still pending in the United States District Court for the Eastern District of New York. For a status update, see the U.S. District Court Civil Docket for the *Abidor* case at: http://dockets.justia.com/docket/new-york/nyedce/1:2010cv04059/308557/.

[10] *See* Abidor Complaint, *supra* not 4, at 8.

[11] *Id.*

[12] According to Abidor, the CBP officer "*ordered* Mr. Abidor to enter his password. Mr. Abidor *complied* with the order." *Id.* at 9 (emphasis added).

[13] *Id.*

[14] *See id.* at 9-10. According to Abidor, the "officers *ordered* Mr. Abidor to write down his password. Mr. Abidor *complied* with this order." *Id.* at 9 (emphasis added). In contrast, the U.S. Department of Justice asserts, "The CBP officers *asked* Abidor to write down the password for his laptop . . . ." Def's Mem. of Law in Supp. of Mot. to

retained his laptop and external hard drive.[15] He was given a "Detention Notice and Custody Receipt for Detained Property" that indicated the devices were being held by ICE.[16] The devices were returned eleven days later after Abidor's attorney contacted authorities on his behalf.[17] Abidor examined his laptop after it was returned and concluded that "the casing and warranty seal [had been] broken open" and that "officers from ICE, CBP and/or other agencies had examined basic directory folders on his laptop such as 'library' and 'users,' as well as backup documents that he had stored on his external hard drive."[18] According to Abidor's complaint, Abidor continues to cross the border for academic purposes and is repeatedly questioned about this incident.[19]

In his complaint, Abidor asserts that current CBP and ICE policies violate the Fourth Amendment (and First Amendment) because they allow "suspicionless search, copying, and detention of electronic devices containing expressive, protected materials."[20] Furthermore, present policies authorize the search even if the owner of the device is not present.[21] Additionally, the policies "permit border officials, without any suspicion of wrongdoing, to detain a traveler's electronic devices, or copies of the contents thereof, for the purpose of further reading and analysis even after the traveler has left the border."[22] Under certain circumstances, CBP and ICE may share this information "with other government agencies or third parties even where there is no suspicion of wrongdoing."[23]

Dismiss at 9, Abidor v. Napolitano, No. CV10-4059 (E.D.N.Y. Jan. 28, 2011) (emphasis added).

[15] *See* Abidor Complaint, *supra* note 4, at 11.

[16] *Id.*

[17] *See id.* at 12.

[18] *Id.*

[19] *See id.* at 13-14. This Article will not explore whether Pascal Abidor, or the other plaintiffs, have standing to obtain the declaratory and injunctive relief that they seek. While standing is clearly an issue in the United States District Court, this Article will assume, *arguendo*, that the plaintiffs have standing, and will only explore the merits of the Fourth Amendment concerns.

[20] *Id.* at 33.

[21] *See id.* at 5.

[22] *Id.*

[23] *Id.*

While it is unclear what direction this case will go, the problem is apparent: International border searches of electronic devices have the potential to seriously impact the personal and professional privacy of individuals. In granting a motion to suppress child pornography obtained from a laptop during a suspicionless search at the border, the U.S. District Court in *United States v. Arnold*[24] stated the concern well:

> Fourth Amendment protection extends to the search of this type of personal and private information at the border. While not physically intrusive as in the case of a strip or body cavity search, the search of one's private and valuable personal information stored on a hard drive or other electronic storage device can be just as much, if not more, of an intrusion into the dignity and privacy interests of a person. This is because electronic storage devices function as an extension of our own memory. They are capable of storing our thoughts, ranging from the most whimsical to the most profound. Therefore, government intrusions into the mind—specifically those that would cause fear or apprehension in a reasonable person—are no less deserving of Fourth Amendment scrutiny than intrusions that are physical in nature.[25]

II. VARIOUS LOWER COURT CASES

Lower courts have had the opportunity in the recent past to consider the constitutionality of the border search exception in the context of electronic devices. This Section will briefly discuss some important lessons obtained from a review of various lower court cases.[26]

---

[24] 454 F. Supp. 2d 999, 1003 (C.D. Cal. 2006) (holding that officers needed reasonable suspicion to search the laptop and that, since reasonable suspicion was not present, the search violated the Fourth Amendment).

[25] *Id.* at 1000-01. The U.S. Court of Appeals for the Ninth Circuit reversed, holding that, based on a review of the U.S. Supreme Court border search cases, "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008), *cert. denied*, 129 S. Ct. 1312 (2009).

[26] The following cases were examined: *United States v. Cotterman*, 637 F.3d 1068 (9th Cir. 2011); *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008); *United States v. Irving*, 452 F.3d 110 (2d Cir. 2006); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005); *United States v. Hanson*, No. CR 09-00946 JSW, 2010 WL 2231796 (N.D. Cal. June 2,

A. General Lessons

All of the cases reviewed involve crimes pertaining to child sexual abuse or child pornography. One researching international border searches of electronic devices will find that the large majority of cases involve child pornography—it is the rare case that involves *any* crime other than child pornography.[27] Not surprisingly, possibly due to the presence of the child pornography, none of the cases reviewed ultimately suppressed the evidence that was found in the assorted electronic devices.

Child pornography is not involved in the case of Pascal Abidor. Abidor is an academic and his data relates to Islamic studies.[28] Breaking from the category of child pornography, it is reasonable to think of many other kinds of data that could theoretically be located on an electronic device at the border: protected trade secrets, material to be published, attorney-client privileged material, and deeply personal information like tax returns and banking information. Should the fact that Abidor's case does not involve child pornography mean it should be treated differently at the border? At a minimum, it might invite greater scrutiny by a court.

Many of the cases discussed "routine" versus "non-routine" border searches, noting that "routine" searches do not require any suspicion while "non-routine" searches generally require some kind of individualized suspicion. Most of the cases, however, avoided this question, simply finding that reasonable suspicion

---

2010) (designated "not for citation"); *United States v. Stewart*, 715 F. Supp. 2d 750 (E.D. Mich. 2010); *United States v. Rogozin*, No. 09-CR-379(S)(M), 2010 U.S. Dist. LEXIS 121162 (W.D.N.Y. Nov. 16, 2010); *Cancel-Ríos v. United States*, No. 10-1386, 2010 U.S. Dist. LEXIS 90336 (D.P.R. Aug. 30, 2010); *United States v. Bunty*, 617 F. Supp. 2d 359 (E.D. Pa. 2008); *United States v. Verma*, No. H-08-699-1, 2010 U.S. Dist. LEXIS 34559 (S.D. Tex. Apr. 8, 2010); *United States v. Pickett*, No. 07-0374, 2008 WL 4330247 (E.D. La. Sept. 16, 2008); *United States v. McAuley*, 563 F. Supp. 2d 672 (W.D. Tex. 2008), *aff'd*, No. 10-50470, 2011 U.S. App. LEXIS 6801 (5th Cir. Mar. 31, 2011); *United States v. Hampe*, No. 07-3-BW, 2007 WL 1192365 (D. Me. Apr. 18, 2007), *aff'd*, 2007 WL 1806671 (D. Me. June 19, 2007); and *United States v. Furukawa*, No. 06-145, 2006 U.S. Dist. LEXIS 83767 (D. Minn. Nov. 16, 2006).

[27] *See, e.g.*, United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007) (stating that in context of ecstasy-importation scheme, searches of "[d]ata storage media and electronic equipment" are included in routine border searches without any suspicion).

[28] *See* Abidor Complaint, *supra* note 4, at 8.

existed under the facts.[29] In at least one case, in denying the motion to suppress the child pornography images found by CBP agents in various electronic storage devices, the court held that even though reasonable suspicion was present justifying the search, reasonable suspicion was not necessary.[30] Some of the courts simply held that searching electronic devices is routine and requires no suspicion.[31] Finally, while not ruling for the

---

[29] *See, e.g.*, United States v. Irving, 452 F.3d 110, 123-24 (2d Cir. 2006) (noting that "routine" searches of "a person's luggage or personal belongings" do not require any individualized suspicion and that a "border search is valid under the Fourth Amendment, even if non-routine, if it is supported by reasonable suspicion," and affirming the district court's decision to deny the motion to suppress the child sexually explicit material found on diskettes in the luggage because the search was supported by reasonable suspicion); United States v. Rogozin, No. 09-CR-379(S)(M), 2010 U.S. Dist. LEXIS 121162, at *9 (W.D.N.Y. Nov. 16, 2010) (The U.S. Magistrate Judge chose not to make a finding regarding whether the search was routine, and instead found under the facts that reasonable suspicion existed "which would justify examining the laptop during the secondary inspection."); United States v. Verma, No. H-08-699-1, 2010 U.S. Dist. LEXIS 34559, at *12 (S.D. Tex. Apr. 8, 2010) (noting that even if deemed "non-routine," facts supported presence of reasonable suspicion); United States v. Hampe, No. 07-3-BW, 2007 WL 1192365, at *4 (D. Me. 2007), *aff'd*, 2007 WL 1806671 (D. Me. 2007) (holding that search of laptop was routine search requiring no suspicion but even if it was deemed non-routine reasonable suspicion was present); United States v. Furukawa, No. 06-145, 2006 U.S. Dist. LEXIS 83767 (D. Minn. Nov. 16, 2006) (adopting the recommendation of the U.S. Magistrate Judge, but not concluding whether a search of electronic devices is routine or not; instead, the court simply stated reasonable suspicion for the search was present, so the motion to suppress was properly denied).

[30] *See* United States v. Bunty, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008) ("Defendant has not pointed to any aspect of the . . . border search that would distinguish it from other routine computer searches at the border.").

[31] *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1008 n.2 (9th Cir. 2008) (holding that, based on a review of the United States Supreme Court border search cases, "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border"); Cancel-Ríos v. United States, No. 10-1386, 2010 U.S. Dist. LEXIS 90336, at *9 (D.P.R. Aug. 30, 2010) (denying habeas corpus petition and holding that Cancel-Ríos could not have prevailed on a motion to suppress evidence of child pornography found by CBP agents on a cell phone and had effective assistance of counsel because "[i]n the context of a border search, a warrantless, suspicionless search of property ordinarily will not run afoul of the owner's Fourth Amendment rights"); United States v. Verma, No. H-08-699-1, 2010 U.S. Dist. LEXIS 34559, at *11 (S.D. Tex. Apr. 8, 2010) (denying the motion to suppress child pornography images taken from a CD by ICE agents and holding that the search did not need any individualized suspicion because it was "routine"; a search is routine as long as it did not "invade Verma's body or damage his computer"); United States v. McAuley, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008) (holding laptops are not "per se embarrassing" and are part of a routine border search, meaning reasonable

defendant, some courts have considered whether First Amendment considerations should impact on Fourth Amendment reasonableness analysis.[32]

Can the court jump right to reasonable suspicion with *Abidor*? Assuming the facts alleged in the complaint are accurate, the agents might have a "hunch" regarding criminal activity, but seemingly no reasonable suspicion of criminal activity. He did not appear nervous, was very cooperative, and only had images of Hamas and Hezbollah rallies. If reasonable suspicion was not present, was the conduct of the agents in the initial seizure and search of the laptop, as well as any later searches, constitutional? Should the agents' conduct be subjected to greater scrutiny given the First Amendment implications?

B. Transportation and Examination of Electronic Devices Beyond the Actual Border

Some courts have voiced concern with the length of time agents possessed the electronic devices after the initial seizure at the border. In *United States v. Stewart*, agents randomly chose Stewart for questioning upon his return flight from Asia.[33] His uncooperative behavior led to a secondary search of his belongings, including two laptops, a digital camera, and three computer memory sticks.[34] Although the camera and memory sticks contained no contraband, the first laptop contained approximately a dozen photographs depicting child pornography.[35] The second laptop had a dead battery and authorities determined that they did not have the means to search it at the airport—

---

suspicion is not required), *aff'd*, No. 10-50470, 2011 U.S. App. LEXIS 6801 (5th Cir. Mar. 31, 2011) (holding that because McAuley voluntarily consented to the search, there was no need to evaluate border search question).

[32] *See* United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005) ("Particularly in today's world, national security interests may require uncovering terrorist communications, which are inherently 'expressive.'") (noting that there has never been a First Amendment exception to the warrant requirement and, therefore, no First Amendment exception to border search); *Arnold*, 533 F.3d at 1010 (dismissing summarily Arnold's First Amendment argument and stating that "despite Arnold's arguments to the contrary we are unpersuaded that we should create a split with the Fourth Circuit's decision in *Ickes*").

[33] 715 F. Supp. 2d 750 (E.D. Mich. 2010).

[34] *Id.* at 751

[35] *Id.*

requiring them to send both laptops to ICE headquarters about twenty miles away for a forensic search the following day.[36]

Stewart did not contend that the initial search of the laptops violated the Fourth Amendment, but rather argued that the evidence obtained from them should be suppressed because the continued retention of the computers and transport to a distant location was unreasonable.[37] The court agreed that this action by authorities was more invasive than a routine border search, but stated there was no Fourth Amendment violation because there was reasonable suspicion that the computer contained contraband based upon the images found on the first laptop during the initial search.[38] This reasonable suspicion rendered the further detention and transport of the computer constitutional.[39]

In *United States v. Rogozin*, Rogozin, a German citizen with lawful permanent residency in New York, was returning to New York from Canada.[40] He indicated to agents that he had visited Niagara Falls overnight as a tourist.[41] The CBP officer found his demeanor to be suspicious because his responses were hesitant, he did not maintain eye contact, and he had traveled all the way from Brooklyn for a one day stay in Canada.[42] The secondary inspection of Rogozin's laptop, camera, iPhone, and video recorder revealed photographs of small children in "sexually suggestive positions."[43] ICE agents then arrived to do a more extensive search of the electronic devices. In reviewing the laptop, the ICE agents "saw some images of naked children, and others in provocative poses."[44]

---

[36] *See id.* at 751-52.

[37] *See id.* at 753. Stewart contended that seizing the computer at the border and then transporting it to another location was "the equivalent of an extended border search that required justification by some level of government suspicion, which was not present in this case." *Id.* at 752. Courts that have utilized the concept of "extended border searches" have generally held that searches that are "removed in time and place from the actual border" are justified by reasonable suspicion that the subject of the search was involved in some kind of criminal conduct. *Id.* at 754 (citing United States v. Guzman-Padilla, 573 F.3d 865, 877-78 (9th Cir. 2009); United States v. Niver, 689 F.2d 520, 526 (5th Cir. 1982)).

[38] *See id.* at 754-55.

[39] *Id.*

[40] No. 09-CR-379(S)(M), 2010 U.S. Dist. LEXIS 121162 (W.D.N.Y. Nov. 16, 2010).

[41] *See id.* at *2.

[42] *Id.* at *3.

[43] *Id.*

[44] *Id.* at *5.

In an interview, Rogozin told the agents that he had seen child pornography on his computer.[45]

The agents decided to retain the laptop and other devices for a forensic examination, and Rogozin was allowed to enter the United States.[46] Four days later, ICE agents conducted a forensic examination of the laptop and discovered 185 photographs of "pretty obvious" child pornography.[47] The agents subsequently obtained a search warrant for the laptop but not for the camera, video recorder or iPhone.[48] Agents arrested Rogozin in his home in Brooklyn approximately two and a half months after the border stop.[49] It appears from the case that none of the electronic devices were returned during the two and a half month period.

The court noted that it "need not decide whether or not the search of the laptop computer can be considered 'routine'" because Rogozin's demeanor at the initial interview, including failure to maintain eye contact, created reasonable suspicion to search the computer.[50] According to the court, the initial discovery of the suggestive photos justified the more detailed search four days later and "[t]he four-day delay between the initial inspection . . . and the follow-up inspection . . . does not invalidate the search."[51] As the results of the second search properly led to probable cause for the warrant for the laptop, the court denied the motion to suppress the evidence obtained from the laptop.

On the other hand, the court did suppress the evidence obtained from the video recorder, iPhone, and camera. Noting that the initial search did not reveal child pornography, the court stated that the "government offers no legitimate excuse [for] continuing to hold the video recorder for this length of time

---

[45] *Id.*

[46] *Id.* at *6.

[47] *Id.* at *3.

[48] Is it significant that the agents, sua sponte, chose to obtain a search warrant? If they did not need to, why did they? Does it indicate that they were merely acting cautiously? Or might it indicate that the agents were acting to avoid a violation of the Constitution in holding the laptop too long? In other cases, agents acted similarly in obtaining a warrant. *See, e.g.*, United States v. Pickett, No. 07-0374, 2008 WL 4330247 (E.D. La. Sept. 16, 2008) (agents could not easily view images on the laptop, thus, they obtained a search warrant to do a more detailed search).

[49] *See Rogozin*, 2010 U.S. Dist. LEXIS 121162, at *3.

[50] *Id.* at *9.

[51] *Id.* at *9-10.

without seeking a warrant."[52] While the initial border search of these items did demonstrate sexually suggestive photographs of children, none of the photographs found were truly pornographic and, therefore, not illegal. Thus, the judge found that the continued seizure of these items was inappropriate, and thus any evidence from the video recorder, I-phone, and camera was inadmissible.[53]

In *United States v. Cotterman*, the Ninth Circuit held that a search of a laptop that lasted two days and encompassed 170 miles was nevertheless protected by the border search exception to the Fourth Amendment.[54] This reversed the district court's decision, which had ruled to exclude hundreds of pornographic images of children found on the defendant's laptop, including photos of the defendant molesting children.[55]

Cotterman's past criminal convictions for sexual crimes against children prompted customs officials to perform a secondary search when he crossed the Mexican border into Lukeville, Arizona.[56] Officers found two laptops and three digital cameras in his vehicle, but the files were password-protected.[57] Officers transferred the devices to Tucson, and two days later, the illegal images were located.[58]

Cotterman did not dispute the validity of the border search exception or its application to the initial search at the border, but argued that the search in Tucson required reasonable suspicion. The court characterized the issue and its holding as follows: "The sticking point is whether the inherent power of the Government to subject incoming travelers to inspection before entry also permits the Government to transport property not yet cleared for entry away from the border to complete its search. Cotterman claims

---

[52] *Id.* at *11. As for the camera and iPhone, the court noted that the record does not clearly indicate whether they are "still in the government's possession." *Id.* at *11 n.6.

[53] *See id.* at *12. Similarly, in *United States v. Hanson*, the court held that holding a laptop for five months after the initial border seizure in order to do a more detailed forensic examination required a search warrant. No. CR 09-00946 JSW, 2010 WL 2231796 (N.D. Cal. June 2, 2010) (designated "not for citation").

[54] 637 F.3d 1068 (9th Cir. 2011).

[55] *Id.* at 1070.

[56] *Id.* at 1071.

[57] *Id.*

[58] *See id.* at 1072.

that it does not. We cannot agree."[59] Despite the physical distance and lapse of time, the court held that this was one continuous search, beginning at the border. Noting that the "border search doctrine is guided—like all Fourth Amendment jurisprudence—by reason and practicality, not inflexible rules of time and space,"[60] the court held that no individualized suspicion is necessary and that "[s]o long as property has not been officially cleared for entry into the United States and remains in the control of the Government, any further search is simply a continuation of the original border search—the entirety of which is justified by the Government's border search power."[61] Further noting, however, that these types of searches need to be analyzed on a "case-by-case basis to determine whether the scope or duration of the intrusion was constitutionally unreasonable,"[62] the court was careful to emphasize that in effectuating the border search the government does not have "carte blanche at the border to do as it pleases absent any regard for the Fourth Amendment."[63]

The initial search of Abidor's laptop merely demonstrated his research material on Islam and jihadists, which can be legally possessed. The images of Hezbollah rallies are no worse than the sexually suggestive images of children that did not technically constitute child pornography found on Rogozin's video recorder, iPhone, and camera. Should the laptop have been immediately returned to Abidor?

Abidor has a stronger argument than both Stewart and Cotterman regarding the transport and detention of both himself and his electronic devices. Abidor and his belongings were transported from the train station to Service-Port Champlain for further questioning, which the complaint states is "far-away" from the Amtrak station.[64] After several hours of questioning in a small

---

[59] *Id.* at 1076.

[60] *Id.*

[61] *Id.* at 1079. Based upon language provided by the United States Supreme Court in past cases, the court listed three instances in which reasonable suspicion may be necessary for searches at the border: (1) highly intrusive searches of the person, (2) highly destructive searches of property, and (3) particularly offensive searches. According to the court, Cotterman's search did not fit into any of the categories. *Id.* at 1079-82.

[62] *Id.* at 1083.

[63] *Id.* at 1079.

[64] Abidor Complaint, *supra* note 4, at 15.

cell and Abidor's subsequent release, Abidor's laptop was then held for an additional eleven days. This is seemingly much more intrusive than the detention of Stewart's and Cotterman's electronic devices. The *Stewart* court mentioned that Stewart could have made the argument that the detention of his laptops was in essence a "full blown seizure requiring probable cause."[65] Should the court entertain the argument that the detention of his electronic devices was such a "full-blown seizure" that the agents needed reasonable suspicion or even probable cause to continue to hold those devices? Using the "case-by-case" basis referenced in *Cotterman*, is the *Abidor* case the one where the Supreme Court will draw the line on reasonableness?

III. WHAT HAS THE U.S. SUPREME COURT HELD REGARDING BORDER SEARCHES? ANY GUIDANCE FROM NON-BORDER SEARCH CASES?

A. Border Search Cases

As the Ninth Circuit in *Cotterman* aptly noted: "We need not dwell long on the general scope of the Government's border search power. It is well-established that the sovereign need not make any special showing to justify its search of persons and property at the international border."[66] Much has been written about the Supreme Court cases discussing searches at the border,[67] so this Section will only highlight a few key points from those cases.

As a general matter, no suspicion is necessary to do a typical search of a person or property at the border. As the Court stated over thirty years ago in *United States v. Ramsey*,[68] in the context of a customs inspection of mail:

> [S]earches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this

---

[65] United States v. Stewart, 715 F. Supp. 2d 750, 755 (E.D. Mich. 2010).

[66] *Cotterman*, 637 F.3d at 1074 (citing United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004)).

[67] *See, e.g.*, Symposium, *The Fourth Amendment at the International Border*, 78 MISS. L.J. i, i-430 (2008); *Warrantless Searches and Seizures,* 39 GEO. L.J. ANN. REV. CRIM. PROC. 43, 117-23 (2010).

[68] 431 U.S. 606 (1977).

> country, are reasonable simply by virtue of the fact that they occur at the border. . . . Border searches, then, 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.[69]

In *United States v. Montoya de Hernandez*,[70] Customs agents "reasonably suspect[ed] that the traveler [was] smuggling contraband in her alimentary canal."[71] The agents held her for sixteen hours until she expelled eighty-eight balloons of cocaine.[72] Recognizing that this is not a routine matter at the border, the Court indicated that the detention was appropriate because the "facts, and their rational inferences, known to [the] customs inspectors . . . clearly supported a reasonable suspicion that respondent was an alimentary canal smuggler."[73] Given the substantial national interest in preventing drugs from entering the country, the Court held "that the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary canal."[74]

Does *Montoya de Hernandez* have some direct application to Abidor's situation?[75] Is holding a person for sixteen hours to wait

---

[69] *Id.* at 616, 619.

[70] 473 U.S. 531 (1985).

[71] *Id.* at 541.

[72] *Id.* at 532-33.

[73] *Id.* at 542.

[74] *Id.* at 541.

[75] *See* Jennifer M. Chacon, *Border Searches of Electronic Data,* LexisNexis Expert Commentary, 2008 EMERGING ISSUES 2430 (June 2008) ("In *United States v. Montoya de Hernandez*, the Court found that the search of a traveler's 'alimentary canal,' achieved by detaining the traveler for sixteen hours until she passed the drugs that she had ingested, could not be conducted in the absence of individualized suspicion.

for a bowel movement the equivalent of holding a person for several hours in a small cinder block cell, requiring that person to provide the password so that agents can look at the laptop, then holding that laptop for eleven days? Abidor may argue that, when examined as a whole, the conduct of the CBP agents was particularly intrusive and should require reasonable suspicion (and that the CBP agents did not have reasonable suspicion). Abidor could argue that the detaining of a computer for eleven days and searching that computer is no different than holding a person for sixteen hours while waiting for a bowel movement.

The *Montoya de Hernandez* Court goes on to state: "It is also important to note what we do *not* hold. Because the issues are not presented today, we suggest no view on what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches."[76] The Court's usage of the phrase "such as" suggests that the "nonroutine" border searches are not limited to strip, body cavity, or x-ray searches—they could decide to include the search of electronic devices like a laptop.[77]

The Court in *Montoya de Hernandez*, however, did not specifically indicate that any level of suspicion was required for more intrusive searches of a person. In *United States v. Flores-Montano*, the Court intimates that some level of suspicion would be required.[78] In *Flores-Montano*, a person with a 1987 Ford Taurus wagon wanted to enter California from Mexico.[79] After referral to secondary inspection, a mechanic under contract with the government disassembled the gas tank within one hour and found thirty-seven kilograms of marijuana.[80] The Court upheld the suspicionless search of the gas tank, noting: "But the reasons that might support a requirement of some level of suspicion in the

---

Instead, the Court found that the dignity and privacy interests at stake required that such searches be conducted only where government officials had 'reasonable suspicion' of criminal activity…. This is the legal context in which border laptop searches have unfolded.").

[76] *Montoya de Hernandez,* 473 U.S. at 541 n.4.

[77] In *United States v. Flores-Montano*, the Court rejected the idea of creating a balancing test based on the "routine" and "nonroutine" framework, indicating that these are only "descriptive term[s] in discussing border searches." 541 U.S. 149, 152 (2004).

[78] *Id.*

[79] *Id.* at 150.

[80] *Id.* at 150-51.

case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles."[81]

Abidor will likely argue that the search of his laptop is more like the "highly intrusive searches of the person" and not like the gas tank search in *Flores-Montano*. As such, it is entitled to greater protection and requires, at a minimum, reasonable suspicion. The government will likely respond by arguing that a search of a computer, a piece of property outside of the body, cannot be compared to a highly intrusive search of the person. *Flores-Montano* has already set the precedent that a highly intrusive search of a vehicle's gas tank, a mere piece of property, does not require individualized suspicion.

The *Flores-Montano* Court goes on to make some open-ended statements that have surfaced in lower court cases discussing searches of electronic devices at the border.[82] Regarding border searches conducted in a "particularly offensive manner," the Court states: "We again leave open the question 'whether, and under what circumstances, a border search might be deemed "unreasonable" because of the particularly offensive manner it is carried out.'"[83] As for "destructive" searches, the Court notes: "While it may be true that some searches of property are so destructive as to require a different result, this was not one of them."[84]

Abidor may be able to fit the search of his laptop into one of these two narrow exceptions.[85] In *Arnold* and *Cotterman*, the Ninth Circuit rejected such an attempt in the context of laptops.[86] Both cases, however, involved child pornography and clear evidence that crime was discovered right at the border or within

---

[81] *Id.* at 152.

[82] *See, e.g.*, United States v. Cotterman, 637 F.3d 1068, 1079-82 (9th Cir. 2011); United States v. Arnold, 533 F.3d 1003, 1007-11 (9th Cir. 2008).

[83] United States v. Flores-Montano, 541 U.S. 149, 154-55 n.2 (citing United States v. Ramsey, 431 U.S. 606, 618 n. 13 (1977)).

[84] *Id.* at 155-56.

[85] *See* Erick Lucadamo, *Reading Your Mind at the Border: Searching Memorialized Thoughts and Memories on Your Laptop and United States v. Arnold*, 54 VILL. L. REV. 541, 572 (2009) ("[I]n the border search context, courts should analyze a laptop as an object, subject only to the two exceptions laid out by the *Flores-Montano* Court, i.e., those searches that are destructive of and particularly offensive to property.").

[86] *Cotterman*, 637 F.3d at 1079-82; *Arnold*, 533 F.3d at 1007-10.

two days of the initial border stop. In the *Abidor* case, in contrast, the crime, if any, was some kind of terrorist-related activity, and no evidence of such crime was uncovered at the border or during the eleven days that Abidor's computer was held. Even if Abidor concedes that his laptop is property (and not analogous to a highly intrusive search of a person) and that the search of his laptop was not destructive, was the search carried out in a particularly offensive manner? Is the *Abidor* case the kind of situation envisioned by the Ninth Circuit when they implied that a search of a laptop could be "constitutionally unreasonable" based upon "the scope or duration of the intrusion"?[87] Might the Supreme Court agree?

B. Non-Border Search Cases

In *United States v. Martinez-Fuerte*, a decision concerning the use of vehicle checkpoints near the Mexican border, the Court provides some further guidance on concerns applicable in a border search context.[88] In *Martinez-Fuerte*, the Court did not interpret the border search exception. Instead, the Court analyzed the checkpoint under its government interest versus degree of intrusiveness (reasonableness) balancing test frequently used to interpret "special needs" types of searches. In affirming the use of the checkpoint utilized for the purpose of detecting illegal aliens, the Court noted:

> A requirement that stops on major routes inland always be based on reasonable suspicion would be impractical because the flow of traffic tends to be too heavy to allow the particularized study of a given car that would enable it to be identified as a possible carrier of illegal aliens. In particular, such a requirement would largely eliminate any deterrent to the conduct of well-disguised smuggling operations, even though smugglers are known to use these highways regularly.[89]

Is the *Martinez-Fuerte* language relevant to Abidor's case and the search of laptops at the border? The "traffic" and "deterrent"

---

[87] *Cotterman,* 637 F.3d at 1083.

[88] 428 U.S. 543 (1976).

[89] *Id.* at 557.

concerns are also applicable at the border.[90] *Martinez-Fuerte* does not extend much protection to Abidor because it suggests that the sheer volume of traffic at a border makes any requirement of reasonable suspicion wholly impractical. Moreover, the Court's concern about the impact that a reasonable suspicion requirement would have on any deterrent effect suggests the Court is disinclined to eliminate or restrict investigative techniques that might have a meaningful deterrent effect on crime.

United States v. Place[91] also provides some guidance. In *Place*, Miami federal agents called New York federal agents and relayed information establishing reasonable suspicion that Place was flying into New York with illegal drugs on a Friday afternoon.[92] The New York agents stopped Place upon arrival at the airport and seized his luggage but allowed him to go on his way.[93] They then took the luggage to another airport across town for a dog sniff, which was positive as to one of the bags of luggage.[94] It took approximately ninety minutes from the initial seizure of the bag until the dog sniff.[95] Due to the late hour on Friday, officers held the bags until Monday when a warrant was obtained for the luggage. The agents found cocaine during the execution of the warrant.[96]

---

[90] *See* David Shipler, *Can You Frisk a Hard Drive?*, N.Y. TIMES, Feb. 19, 2011,at WK5, *available at* http://www.nytimes.com/2011/02/20/weekinreview/20laptop.html?_r=1 ("If you stand with the Customs and Border Protection officers who staff the passport booths at Dulles airport near the nation's capital, their task seems daunting. As a huge crowd of weary travelers shuffle along in serpentine lines, inspectors make quick decisions by asking a few questions (often across language barriers) and watching computer displays that don't go much beyond name, date of birth and codes for a previous customs problem or an outstanding arrest warrant. The officers are supposed to pick out the possible smugglers, terrorists or child pornographers and send them to secondary screening. The chosen few—6.1 million of the 293 million who entered the United States in the year ending Sept. 30, 2010—get a big letter written on their declaration forms: A for an agriculture check on foodstuffs, B for an immigration issue, and C for a luggage inspection. Into the computer the passport officers type the reasons for the selection, a heads-up to their colleagues in the back room, where more thorough databases are accessible.").

[91] 462 U.S. 696 (1983).

[92] *Id.* at 698.

[93] *Id.* at 699.

[94] *Id.*

[95] *Id.*

[96] *See id.* at 698-99.

Notably, the Court held that seizure of a traveler's luggage is "tantamount to seizure of the person."[97] Applying the *Terry v. Ohio*[98] balancing of interests approach (balancing the government interest with the degree of intrusion),[99] the *Place* Court held that the law enforcement conduct "exceeded the permissible limits of a *Terry*-type investigative stop."[100] While *Terry* permitted law enforcement to seize Place and his luggage in a limited way based merely upon reasonable suspicion, the conduct of the agents here rose to a higher level requiring probable cause. Since probable cause was not present, the seizure was "unreasonable."[101] The length of the detention of the bags until the dog sniff—ninety minutes—was not reasonable given that the agents failed to act diligently when they could have. They knew that the defendant was coming to New York and they could have had the dog at the airport of arrival. While the Court "decline[d] to adopt any outside time limitation," the ninety-minute period here was too long.[102]

In evaluating whether a legally permissible reasonable suspicion limited seizure had converted into a more significant seizure requiring probable cause, the *Place* Court emphasized (1) the movement of the luggage, (2) the length of the detention of the luggage, and (3) whether law enforcement diligently pursued their investigation.[103] How do those concerns apply in the context of the eleven-day seizure and retention of Abidor's laptop? Significantly, the *Place* case does not occur at the border.[104] As such, the Court might simply decide that the case is wholly inapplicable. If they do consider *Place*, however, it helps Abidor in several ways. First, the *Place* Court treated the seizure of the luggage as "tantamount to seizure of the person,"[105] which obviously helps Abidor in his argument that seizing and searching his laptop is more akin to a person than it is to property. Second, whereas *Place* viewed the

---

[97] *Id.* at 708 n.8.

[98] 392 U.S. 1 (1968).

[99] *Place,* 462 U.S. at 703.

[100] *Id.* at 709.

[101] *Id.* at 710.

[102] *Id.* at 709.

[103] *See id.* at 707-10; *see also* Florida v. Royer, 103 S. Ct. 1319, 1329 (1983); Dunaway v. New York, 442 U.S. 200 (1979).

[104] *Place,* 462 U.S. at 698.

[105] *Id.* at 708 n.8.

situation as one where the seizure had converted from a reasonable suspicion seizure into a probable cause seizure, Abidor's situation could be viewed as one that progressed from needing no individualized suspicion to needing reasonable suspicion. CBP agents moved the laptop, held it for an extended period of time, and, arguably, did not diligently pursue their investigation.

Lastly, in *City of Ontario, California v. Quon*, the Court considered whether a government employer violated the rights of an employee when the employer read text messages sent and received on a pager the employer issued to the employee.[106] The Court assumed, for argument's sake only, that the employee had a reasonable expectation of privacy over text messages sent on the government-provided pager.[107] Nevertheless, the Court decided that the conduct of the employer, *under the circumstances*, was reasonable.[108]

The *Quon* Court, however, refused to conclude that there is always a reasonable expectation of privacy over electronic communication and devices:

> The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.[109]

Based upon *Quon*, it seems that the Supreme Court will decide questions involving advanced forms of technology on a case-by-case basis. If facing a situation like that presented in *Abidor*, will the Court fully embrace the personal privacy concerns at issue

---

[106] 130 S. Ct. 2619, 2624-26 (2010).
[107] *See id.* at 2628-31.
[108] *See id.* at 2632-33.
[109] *Id.* at 2629-30.

with electronic devices at the border? Or will it figure out a way to resolve Abidor's matter on very narrow grounds (or not review it at all)? Will the fear of "elaborating too fully on the Fourth Amendment implications" of laptop searches at the border chill the Supreme Court? If the decision was up to Justice Scalia, it seems he would face the question directly—regardless of the presence of an advanced form of technology. In his *Quon* concurrence, Justice Scalia urges the Court to draw the digital line:

> Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The Court's implication that where electronic privacy is concerned we should decide less than we otherwise would (that is, less than the principle of law necessary to resolve the case and guide private action) – or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions – is in my view indefensible. The-times-they-are-a-changin' is a feeble excuse for disregard of duty.[110]

Will Justice Scalia be the force that empowers the Court to rule on laptop searches at the border?

IV. OTHER RELEVANT CONSIDERATIONS

A. General Reflections on Justices of the Supreme Court

Analyses of political science databases by the *New York Times* reflect that the Roberts Court "has staked out territory to the right of the two conservative[111] courts that immediately

---

[110] *Id.* at 2635 (Scalia, J., concurring) (citation omitted).

[111] What does "conservative" mean in the context of the *New York Times* article?

> The leading database, created by Harold J. Spaeth with the support of the National Science Foundation about 20 years ago, has served as the basis for a great deal of empirical research on the contemporary Supreme Court and its members. In the database, votes favoring criminal defendants, unions, people claiming discrimination or violation of their civil rights are, for instance, said to be liberal. Decisions striking down economic regulations and favoring prosecutors, employers and the government are said to be conservative.

Adam Liptak, *Court Under Roberts Is Most Conservative in Decades*, N.Y. TIMES, July 25, 2010, at A1, *available at* http://www.nytimes.com/2010/07/25/us/25roberts.html?_r=

preceded it," noting that "[i]n its first five years, the Roberts court issued conservative decisions 58 percent of the time. And in the term ending a year ago, the rate rose to 65 percent, the highest number in any year since at least 1953."[112] The *New York Times* article further notes:

> Four of the six most conservative justices of the 44 who have sat on the court since 1937 are serving now: Chief Justice Roberts and Justices Alito, Antonin Scalia and, most conservative of all, Clarence Thomas. (The other two were Chief Justices Burger and Rehnquist.) Justice Anthony M. Kennedy, the swing justice on the current court, is in the top 10.[113]

As for the additions of Elena Kagan and Sonia Sotomayor, the article notes that "there is no reason to think they will make a difference in the court's ideological balance. Indeed, the data show that only one recent replacement altered its direction, that of Justice Samuel A. Alito, Jr. for Justice Sandra Day O'Connor in 2006, pulling the court to the right."[114]

The current political composition of the Court (five Justices nominated by Republican presidents and four Justices nominated

---

1&scp=1&sq=%22Court%20Under%20Roberts%20is%20most%20conservative%20in%20decades&st=cse.

[112] *Id.*

[113] *Id.*

[114] *Id.*; *see also* Greg Stohr, *Roberts Supreme Court's Partisan Split Shows New Justices Are Predictable,* BLOOMBERG.COM (June 30, 2011, 11:01 PM), http://www.bloomberg.com/news/2011-07-01/roberts-supreme-court-s-partisan-split-shows-new-justices-are-predictable.html ("The newest justices fueled the trend, rewarding the men who appointed them with consistent and predictable votes. President Barack Obama's two choices, Sonia Sotomayor and Elena Kagan, voted in virtual lockstep and usually alongside fellow Democratic appointees Ruth Bader Ginsburg and Stephen Breyer. Former President George W. Bush's two selections, Chief Justice John Roberts and Justice Samuel Alito, voted together more than any other duo."). *But see* Joan Biskupic, *"Dynamic" duo of Kagan, Sotomayor add vigor to court*, USA TODAY (Mar. 1, 2011, 1:46 PM), http://www.usatoday.com/news/washington/judicial/2011-03-01-courtarguments_N.htm ("The new justices have brought a stronger voice on the left than the four liberals had before Sotomayor joined on 2009 and Kagan in 2010. Kagan particularly is putting forward broader legal arguments that could guide her colleagues' thinking, often in contrast to those set up by the court's five conservatives.").

by Democratic presidents)[115] and the studies referenced here suggest that any decision in Abidor's case would favor the government—likely ruling that a laptop is mere property and that it can be searched at the border and beyond without reasonable suspicion. On the other hand, national security concerns do not fall neatly into ordinary political divisions—will politics or ideological perspectives have any impact? While, "by and large, presidents are successful with their appointees" with respect to desired ideological goals,[116] Supreme Court history reveals instances of Justices deciding cases wholly inconsistent with the perspective that the public, and the president who appointed the justices, might have anticipated.[117] The answer is not clear—but it does appear that the present composition of the United States Supreme Court will favor the government in any ruling on searching electronic devices at the border.

B. Perspectives of Justices in Various Oral Arguments

What guidance can be obtained from the questions and comments from the Justices at oral argument? Of course, a Justice's words at oral argument have no persuasive value under the law—but they can be very revealing when speculating how a Justice might respond in future situations. This Section will examine the words of various Justices[118] in the oral arguments

---

[115] *See Biographies of Current Justices of the United States*, UNITED STATES SUPREME COURT, http://www.supremecourt.gov/about/biographies.aspx (last visited Jan. 23, 2012).

[116] LEE EPSTEIN & JEFFREY A. SEGAL, ADVICE AND CONSENT: THE POLITICS OF JUDICIAL APPOINTMENTS 132 (2005).

[117] Bradley W. Joondeph, *Law, Politics, and the Appointment Process*, 46 SANTA CLARA L. REV. 737, 751 (2006) ("Earl Warren and William Brennan had voting records that were much more liberal than the views of Dwight Eisenhower. Byron White was substantially more conservative than John F. Kennedy. Harry Blackmun grew more liberal than Richard Nixon, and David Souter's voting record has likely surprised George H.W. Bush. Nonetheless, '[m]ost justices appointed by conservative presidents cast a high percentage of conservative votes,' while 'most justices appointed by liberal presidents cast a higher percentage of left-of-center votes than their colleagues seated by more conservative presidents.' That is, '[m]ore often than not' justices 'vote in ways that would very much please the men who appointed them.'" (quoting EPSTEIN & SEGAL, *supra* note 116, at 132)).

[118] This Section will not consider the comments or questions of Justice Clarence Thomas because he has not spoken at oral argument in over five years. *See* Adam Liptak, *No Argument: Thomas Keeps 5-Year Silence,* N.Y. TIMES, Feb. 13, 2011, at A1,

from the border search case, *United States v. Flores-Montano*,[119] and the advanced technology case of *City of Ontario, California v. Quon*.[120]

1. *United States v. Flores-Montano*

In *Flores-Montano*, Justice Breyer suggests that he is concerned with the potential for overzealous agents at the border. Consider the following:

> I'm trying to figure out if we have each customs agent for himself to conduct whatever suspicionless searches he wants, and you have a few of the, perhaps in every organization there are a few unusual ones who cause some problems, are there any internal checks within the system, because you're going to not have a judicial check?[121]

Justice Breyer appears to be concerned that there is not enough oversight, especially judicial oversight, with the conduct of federal agents at the border. Does this indicate he might be supportive of requiring law enforcement to have some kind of individualized suspicion to examine the contents of electronic devices at the border? In his concurrence in *Flores-Montano*, he makes note of the fact that CBP keeps records of border searches it conducts (including the reasons for the searches).[122] Will those records satisfy the oversight concerns of Justice Breyer?

In questioning counsel for Flores-Montano, Justice Breyer voices concern with the implications of empowering terrorist

---

available at http://www.nytimes.com/2011/02/13/us/13thomas.html?_r=1 ("A week from Tuesday, when the Supreme Court returns from its midwinter break and hears arguments in two criminal cases, it will have been five years since Justice Clarence Thomas has spoken during a court argument."); *see also* David A. Karp, *Why Justice Thomas Should Speak at Oral Argument*, 61 FLA. L. REV. 611, 612-13 (2009) ("Since 2004, when oral argument transcripts began identifying Justices by name, Justice Thomas has made just eleven comments—while sitting through more than 400 hours of argument.").

[119] 541 U.S. 149 (2004).

[120] 130 S. Ct. 2619 (2010).

[121] Oral Arg. at 22:8-15 United States v. Flores-Montano, 541 U.S. 149 (2004) (No. 02-1794) [hereinafter *Flores-Montano* Oral Argument], *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/02-1794.pdf (last visited Jan. 23, 2012).

[122] *Flores-Montano*, 541 U.S. at 156 (Breyer, J., concurring).

activity if reasonable suspicion is required for disassembly of property:

> [S]uppose there's a terrorism problem and . . . they say that we want to search every fifteenth truck that comes in, there might be anthrax or bombs or whatever and we want to give the agents the power to look thoroughly into these big trucks even without suspicion. Now were you saying the Fourth Amendment would stop that?[123]

Would Justice Breyer be similarly concerned if the "property" in question was a laptop or some other kind of electronic device? The potential for enabling terrorism is present in either situation. How will Justice Breyer and the Court balance terrorist concerns with the privacy of individuals like Pascal Abidor?

Justice Scalia is also concerned with burdening agents at the border: "[T]here are just some intuitions that agents get that may not rise to the level of what a court may acknowledge is an articulable suspicion, and they shouldn't—they shouldn't have to worry about whether they have to prove that or not."[124] Justice Scalia seems to have confidence in the intuition of agents—as such, they should not have to worry about whether or not they have sufficient individualized suspicion. As for the oversight concerns brought up by Justice Breyer, Justice Scalia offers the following comment:

> I mean, it seems to me if you have an agent who repeatedly has a—cars backing up at the—at the gate that—that he's controlling, and who repeatedly comes up empty on—on gas tank searches, that fellow's not going to be there very long. I mean, it, it's easy to observe somebody who's abusing the system, it seems to me.[125]

Justice Scalia appears to think that overzealous federal agents will be rare because the open nature of their job will prevent them from abusing their power. Given his comments, it seems unlikely that Justice Scalia would be sympathetic to any argument presented by Pascal Abidor.

---

[123] *Flores-Montano* Oral Argument, *supra* note 121, at 40:2-10.

[124] *Id.* at 36:4-7.

[125] *Id.* at 37:5-11.

What about Justice Kennedy, often referred to as the "swing vote"[126] with the present Supreme Court? Does he give any indication of his perspective in the *Flores-Montano* oral argument? Consider the following comments:

> If 85 percent of the people with the gas tanks that were searched have the contraband, what you're asking us to do is to protect the expectation of the other 15 percent . . . it seems to me to put the exclusionary rule somewhat into question with reference to the border.[127]

Is Justice Kennedy suggesting that the ends should justify the means? The implication is that the large majority of time the agents get the bad guy—so the remaining fifteen percent of the public should just deal with it. Will Justice Kennedy feel the same way about Pascal Abidor?

2. *City of Ontario, California v. Quon*

What about the Court's comfort level with advanced forms of technology? Might that have an impact on how they constitutionally approach searches at the border when electronic devices are at issue? A review of a few passages from the *Quon* oral argument is revealing.

Consider a few comments and questions of Chief Justice Roberts:

> And I think it might be the better course to say that the Constitution applies, but we're going to be more flexible in

---

[126] *See* Adam H. Morse & Julian E. Yap, *A Panel-Based Supreme Court*, 37 OHIO N.U. L. REV. 23, 34-35 (2011) ("The frequency with which the Court decides cases by a 5-4 vote with at most one or two swing Justices – often O'Connor before her retirement and Kennedy since then—creates a reality that the law, particularly on matters of constitutional law, is frequently whatever one swing Justice says it is. For example, the Court split 5-4 or 6-3 in almost half of the seventy-four signed decisions over the course of the 2008 October Term. Justice Kennedy was in the majority 92% of the time, and, crucially, in all but five of the twenty-three cases that split 5-4." (footnote omitted)); *see also* Erwin Chemerinsky, *When it Matters Most, it is Still the Kennedy Court*, 11 GREEN BAG 2D 427, 427-28 (2008) ("The bottom line is that when the Court is divided 5-4 on issues where there are clear liberal and conservative positions, Justice Kennedy is the swing vote.").

[127] *Flores-Montano* Oral Argument, *supra* note 121, at 50:18-24.

> determining what's reasonable because they are dealing with evolving technology . . . .[128]
>
> . . .
>
> . . . I just don't know how you tell what is reasonable—I suspect it might change with how old people are and how comfortable they are with technology . . . .[129]
>
> . . .
>
> . . . Maybe—maybe everybody else knows this, but what is the difference between a pager and e-mail?[130]

Chief Justice Roberts is obviously wary about giving constitutional status to a particular type of technology because technology changes so fast. What does it mean to "be more flexible in determining what's reasonable because they are dealing with evolving technology"? One could infer from this statement that Justice Roberts thinks law enforcement should be given wider discretion when dealing with advanced forms of technology—after all, since technology is changing so rapidly, it is reasonable for law enforcement in exploring advanced forms of technology to periodically make some reasonable mistakes.

What about his comments regarding age and comfort with technology? Chief Justice Roberts seems to be saying that age and experience can help shape one's perspective on the "reasonableness" of the expectation of privacy in regards to electronic devices. Assuming he is not particularly comfortable with technology, could one expect that he might conclude that a heightened expectation of privacy in an electronic device at the border is not reasonable? Hence, the intrusion on a person like Mr. Abidor is not that high?

What about Chief Justice Roberts's question about the difference between a pager and e-mail—does this offer any

---

[128] Oral Arg. at 23:7-11 City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332) [hereinafter *Quon* Oral Argument], *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf (last visited Jan. 26, 2012).

[129] *Id.* at 24:1-4.

[130] *Id.* at 29:18-20.

guidance? His lack of understanding of technology[131] might impact how bold the Court will be when reviewing new technology in future decisions. He might conclude that the best course of action is to simply leave the issues to the lower courts and let the passage of time resolve the constitutional issues presented by the technology.

Justice Scalia also offers some interesting comments. Recall that the *Quon* case considered whether a public employer violated the rights of an employee when the employer read text messages sent and received on a pager the employer had issued to the employee. In the following passage, Justice Scalia discusses the role of the statute, the Stored Communications Act,[132] in relation to the Fourth Amendment: "[T]hat's why you have the statute, because the Fourth Amendment wouldn't solve the problem, because you are effectively making it public by sending it to somebody whom you don't know is immune from disclosure. So, in order to stop the intermediary from making it public, you needed the statute."[133] Justice Scalia is sending the clear message that the Constitution (specifically, the Fourth Amendment) cannot cover every concern; statutes may be a more appropriate means for fully protecting digital information than the Fourth Amendment. Does this suggest he might want to stay the course with laptops at the border—continuing to allow full searches without any individualized suspicion? Would he leave it to Congress—if they deem it appropriate—to provide more protection to travelers at the border?

---

[131] A thorough review of the *Quon* oral argument reflects that the Court could use some guidance on modern technology and how the various devices work. *See, e.g.*, *id.* at 25:20-23 (Chief Justice Roberts: "So, your—your position would require people basically to have two of these things with them, two whatever they are, text messager or the BlackBerries or whatever, right?"); *id.* at 44:1-5 (Chief Justice Roberts: "What happens, just out of curiosity, if you're—he is on the pager and sending a message and they're trying to reach him for, you know, a SWAT team crisis? Does he—does the one kind of trump the other, or do they get a busy signal?").

[132] Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2011).

[133] *Quon* Oral Argument, *supra* note 128, at 52:14-19.

C. Potential Federal Legislation on Warrantless Border Searches of Electronic Devices

In *Cotterman*, in the context of seizing and later searching a laptop at the border, the Ninth Circuit discussed the role of courts versus the role of Congress or the executive branch:

> We recognize that few legitimate travelers would appreciate being regularly delayed in order to allow the Government to adequately search his or her property. However, our role is to determine what is legal, not what is desirable. We leave to Congress or the Department of Homeland Security the decision to promulgate limits on the utilization of more complex searches through legislation or rulemaking . . . .[134]

In fact, Congress has considered[135] and is considering legislation on warrantless border searches of electronic devices. In January 2011, Representative Loretta Sanchez (D-CA) introduced the Border Security Search Accountability Act of 2011 (2011 Border Security Act).[136] Some interesting aspects of the legislation[137] include:

---

[134] United States v. Cotterman, 637 F.3d 1068, 1077 n.10 (9th Cir. 2011).

[135] In 2008-09, Senator Russ Feingold (D-WI) and Representative Eliot Engel (D-NY) sponsored bills to statutorily require some level of suspicion to search electronic devices at the international border. Securing Our Borders and Our Data Act of 2009, H.R. 239, 111th Cong. (2009); Travelers' Privacy Protection Act of 2008, S. 3612, 110th Cong. (2008). These bills were not presented for a vote during the last session of Congress but demonstrate that Congress has been concerned with electronic border searches for several years. *See also* Carolyn James, *Balancing Interests at the Border: Protecting Our Nation and Our Privacy in Border Searches of Electronic Devices*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 219, 227-30 (2011) (discussing other legislation considered in 2008-09 as well as past and present directives of CBP and ICE). Congress has also passed legislation generally covering border searches. *See, e.g.*, 19 U.S.C. § 482 (2002).

[136] Border Security Accountability Act of 2011, H.R. 216, 112th Cong. (2011) [hereinafter 2011 Border Security Act], *available at* http://pub.bna.com/eclr/hr216 intro.pdf.

[137] A detailed comparison of the 2009 CBP Directive and the 2009 ICE Directive, see *supra* note 7, with the 2011 Border Security Act, is beyond the scope of this Article. Nevertheless, it is worth noting that some of the concerns addressed in this proposed legislation are already covered in the directives. For example, the 2011 Border Security Act would require that searches of electronic devices be done in the presence of a supervisor. The 2009 CBP Directive is in accord with this recommendation. 2009 CBP

- Prohibits confidential information (e.g. medical information) viewed at the border from being shared with other government agencies;[138]
- Searches of electronic devices must be done "in presence of a supervisor and, where appropriate, in the presence of the individuals whose electronic devices are subject to searches";[139]
- Ascertain a set number of days electronic devices can be retained by border officials absent "probable cause";[140]
- Those who have data copied, retained, shared, or entered given written notice unless that hinders a national security investigation;[141]
- Individuals receive receipt if electronic device taken from them;[142]
- Proper training on privacy, civil rights, etc., to each officer conducting searches of electronic devices at the border;[143]
- Auditing mechanism to ensure proper procedure taken for e-device searches.[144]

DIRECTIVE, *supra* note 7, § 5.1.3. The 2009 ICE Directive, however, does not have such a requirement. *See* 2009 ICE DIRECTIVE, *supra* note 7.

[138] 2011 Border Security Act, *supra* note 136, § 2(b)(2).

[139] *Id.* Both the 2009 CBP Directive and the 2009 ICE Directive include language suggesting that the searches be done in the presence of the traveler, but the exceptions to this exception are very broad. *See, e.g.*, 2009 CBP DIRECTIVE, *supra* note 7, § 5.1.4 ("Searches 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."); 2009 ICE DIRECTIVE, *supra* note 7, § 8.1(2) ("If permitting an individual to witness the search itself could reveal law enforcement techniques or potentially compromise other operational concerns, the individual will not be permitted to observe the search.").

[140] 2011 Border Security Act, *supra* note 136, § 2(b)(3).

[141] *Id.* § 2(b)(6).

[142] *Id.* § 2(b)(5).

[143] *Id.* § 3(a).

[144] *Id.* § 3(b). While Congress considers legislation like the 2011 Border Security Act, it simultaneously contemplates laws that go in the opposite direction. *See, e.g.*,

There is clearly some public support to limit the government's role at the border.[145] For example, on May 18, 2011, an advocacy group called The Constitution Project issued a report describing various legal and privacy concerns with DHS's border search policies with regard to electronic devices.[146] Reporters are routinely highlighting the experiences of individuals who have encountered electronic problems at the border.[147] Simultaneously, however, national security interests are highlighted almost

---

David Kravets, *Internet 'Kill Switch' Legislation Back in Play*, WIRED.COM (Jan. 28, 2011), http://www.wired.com/threatlevel/2011/01/kill-switch-legislation/ ("Legislation granting the president internet-killing powers is to be re-introduced soon to a Senate committee . . . . An aide to the Homeland Security committee described the bill as one that does not mandate the shuttering of the entire internet. Instead, it would authorize the president to demand turning off access to so-called 'critical infrastructure' where necessary.").

[145] *See* Alan Charles Raul Washington, Letter to Editor, *Time to Revive Privacy Board to Protect Civil Liberties,* N.Y. TIMES (Nov. 22, 2010), http://www.nytimes.com/2010/11/23/opinion/lweb23privacy.html (In light of "the intrusiveness of laptop searches at the border," the author calls for President Obama to revive the Privacy and Civil Liberties Board which has been vacant since January 2008: "The privacy board was originally enacted in response to a recommendation of the 9/11 Commission to help ensure that the war against terrorism would not compromise the rights of Americans.").

[146] *See* THE CONSTITUTION PROJECT, SUSPICIONLESS BORDER SEARCHES OF ELECTRONIC DEVICES: LEGAL AND PRIVACY CONCERNS WITH THE DEPARTMENT OF HOMELAND SECURITY'S POLICY (2011) [hereinafter THE CONSTITUTION PROJECT], http://www.constitutionproject.org/pdf/Border_Search_of_Electronic_Devices_0518_2011.pdf.

[147] *See, e.g.*, Shahrzad Noorbaloochi, *Legality of Homeland Security Searches of Electronics at Border Questioned*, THE EPOCH TIMES (Feb. 7, 2011), http://www.theepochtimes.com/n2/content/view/50744/ ("David House, 23, of Cambridge, Mass., is an MIT researcher whose laptop, flash drives, and cameras were confiscated at the U.S.-Mexico border by the Department of Homeland Security (DHS) on his way back into the United States after a vacation in Mexico."); Kim Zetter, *Another Hacker's Laptop, Cellphones Searched at Border*, WIRED.COM (Nov. 18, 2010 8:25 PM), http://www.wired.com/threatlevel/2010/11/hacker-border-search ("A well-known and respected computer-security researcher was detained for several hours Wednesday night by border agents who searched his laptop and cell phones before returning them to him."). Zetter's article suggests that some of the people detained might have had a connection to Wiki Leaks. While some might support the publication of top-secret federal government data, as Wiki Leaks promotes, there is arguably a parallel fear that those who facilitate the exposure of such documents on the Internet are a danger to national security. Since websites like Wiki Leaks are dependent upon the passage of information via electronic devices, Congress might experience some strong political pressure to not pass legislation that would afford additional protections at the border.

daily.[148] Is the 2011 Border Security Act the most that can be expected in light of the significant national security interests involved with border searches?[149] Does it sufficiently address the privacy intrusion involved with this type of search?

Notably, the 2011 Border Security Act does not address one of Abidor's main concerns—the detailed search of an electronic device without reasonable suspicion. Neither the 2009 CBP Directive nor the 2009 ICE Directive require individualized suspicion to search electronic devices.[150] One recommendation in The Constitution Project's report urges DHS to "[a]mend the CBP and ICE Directives to require that CBP and ICE officials may not search the content or information contained in electronic devices of U.S. persons unless there exists a reasonable suspicion that the electronic device contains illegal material or evidence of illegal conduct."[151]

The 2011 Border Security Act would require DHS to ascertain a set number of days electronic devices can be retained by border officials absent "probable cause."[152] In contrast, under both the 2009 CBP Directive and the 2009 ICE Directive, agents may detain electronic devices for further review for a "reasonable" period of time.[153] The 2009 CBP Directive specifically states that "[u]nless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days."[154] The 2009 ICE Directive states that "[s]earches are generally to be completed within 30 days of the date of detention, unless circumstances exist that would warrant more time."[155]

---

[148] *See, e.g.*, Eric Schmitt, *Lawmakers Hear of Threat by Domestic Terrorists*, N.Y. TIMES, Feb. 10, 2011, at A14, *available at* http://www.nytimes.com/2011/02/10/us/politics/10terror.html?ref=politics ("'In some ways, the threat today may be at its most heightened state since the attacks nearly 10 years ago,' Janet Napolitano, the secretary of homeland security, told lawmakers.").

[149] As of the writing of this Article, Congress had not acted on this bill after referring it to the House Committee on Homeland Security.

[150] *See* 2009 ICE DIRECTIVE, *supra* note 7, § 6.1; 2009 CBP DIRECTIVE, *supra* note 7, § 5.1.2.

[151] THE CONSTITUTION PROJECT, *supra* note 146, at 11.

[152] 2011 Border Security Act, *supra* note 136, § 2(b)(3).

[153] 2009 ICE DIRECTIVE, *supra* note 7, § 8.3(1); 2009 CBP DIRECTIVE, *supra* note 7, § 5.3.1.

[154] 2009 CBP DIRECTIVE, *supra* note 7, § 5.3.1.

[155] 2009 ICE DIRECTIVE, *supra* note 7, § 8.3(1).

What impact might public opinion and pending legislation have on the courts, and possibly the Supreme Court, when facing facts like that presented in the *Abidor* case? It may motivate the courts to "stay the course," giving law enforcement wide authority at the border as has been the case for decades. If Congress wants to give travelers greater protection than the Supreme Court's interpretation of the Constitution requires, it can do so. Courts may choose to dodge the issue and let the legislature address—if they desire to do so—the privacy concerns presented by these border searches.

D. Fourth Amendment and First Amendment Concerns at the Border

In the context of border searches, a high potential exists for conflict between law enforcement authority under the Fourth Amendment and the right to free expression under the First Amendment. The Court, however, has not been very sympathetic to First Amendment concerns at the border, as noted in the 1972 *Ramsey* decision: "More fundamentally, however, the existing system of border searches has not been shown to invade protected First Amendment rights . . . ."[156] The Court's comments in *Ramsey—focusing* on the "existing system of border searches"—seem to leave open the possibility that the Court might consider the First Amendment concerns under a *different* system of border searches.[157] Do border searches of electronic devices present that opportunity? As one academic authority noted in 2010:

---

[156] United States v. Ramsey, 431 U.S. 606, 623 (1977).

[157] *See* Timothy Zick, *Territoriality and the First Amendment: Free Speech at—and Beyond—Our Borders*, 85 NOTRE DAME L. REV. 1543, 1568 (2010) ("In *United States v. Ramsey*, the Supreme Court held that the probable cause and warrant requirements did not apply to the opening of incoming international letter-class mail by customs officials. Such searches were deemed reasonable merely by virtue of their location. The *Ramsey* Court summarily dismissed any First Amendment concerns, reasoning that the detailed regulatory restrictions on opening letter mail negated any concern regarding the chilling of expression. 'Accordingly,' the Court said, 'we find it unnecessary to consider the constitutional reach of the First Amendment in this area in the absence of the existing statutory and regulatory protection.' *Ramsey* thus declined an invitation to de-territorialize constitutional scrutiny of border searches involving expressive materials. The invitation has recently been proffered anew—and again declined—in cases involving more modern forms of communication.").

> The era of the personal computer has raised some new concerns regarding the territorial First Amendment. In a globalized society, international travelers routinely carry computing devices, which are typically filled with expressive material, at the border. The question has arisen whether the First Amendment requires an exception to the broad search and seizure authority customs officials possess at the nation's borders. . . . Although most of the constitutional concerns regarding border searches relate to the Fourth Amendment, serious First Amendment issues can also arise. As we have seen, information and ideas flow across the border in many different forms. . . . Laptops and other computing devices now routinely carried by international travelers contain private and expressive material including diaries, medical information, personal correspondence, and financial records. Travelers subjected to warrantless border searches have challenged the searches on both Fourth Amendment and First Amendment grounds.[158]

Despite the Court's apparent lack of concern about First Amendment issues at the border, "[t]ravelers subjected to warrantless border searches have challenged the searches on both Fourth Amendment and First Amendment grounds."[159] In general, however, lower courts have chosen not to recognize any First Amendment exception to the broad border search authority.[160] To hold otherwise, say the lower courts, would "create a sanctuary at the border for all expressive material—even for terrorist plans . . . ." Furthermore, recognizing a First Amendment exception to the border search doctrine would ensure significant headaches for those forced to determine its scope and "[t]hese sorts of legal wrangles are exactly what the Supreme Court wished to avoid by sanctioning expansive border searches."[161]

Given the present state of the law, it appears that any First Amendment claims presented by Abidor are not likely to be well-

---

[158] *Id.* at 1567-68.

[159] *Id.* at 1568.

[160] *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 506-07 (4th Cir. 2005).

[161] *Ickes*, 393 F.3d at 506.

received.[162] The national security concerns and the administrative problems presented by increased scrutiny may simply be too great. Will the same problems limit travelers' Fourth Amendment protections at the border?

E. Frequency of Border Searches of Electronic Storage Devices

Do lawsuits like Abidor's overstate the problems regarding border searches of electronic devices? Is there really a problem with border searches of these devices? It helps to review some raw numbers on actual border searches.

According to Abidor's complaint, "[b]etween October 1, 2008, and June 2, 2010, over 6500 people—nearly 3000 of them U.S. citizens—were subjected to a search of their electronic devices as they crossed U.S. borders."[163] On its face, this seems like a lot of potential privacy intrusions.

The Department of Homeland Security, however, provides a different perspective using very similar numbers:

> For the reporting period October 1, 2009 to April 30, 2010, CBP encountered more than 168.2 million travelers at U.S. ports of entry. Of these travelers, approximately 3.7 million (2.2% of the 168.2 million travelers) were referred for secondary inspection; however, of these 3.7 million travelers, CBP conducted *only* 2,272 searches of electronic media during this time period. A "search" in this regard is broadly defined to include a simple request to turn the device on as a means of ensuring that it is what it purports to be. Detailed information on these searches is only available for those performed on laptops. Of the total number of searches of electronic media, *only* 673 searches of any type were performed on laptops—*just* 0.0184% of

---

[162] *See* Zick, *supra* note 157, at 1570 ("In this context, at least, it is apparent that globalization and digitization have not altered the territorial First Amendment. Expressive interests are enforced differently, if at all, at the territorial borders. Like other border searches, warrantless and suspicionless searches of computing devices have been deemed valid merely by virtue of their location. This is so despite the fact that the search of computing devices is in some cases a more substantial invasion than, say, a search of papers or international mail.").

[163] Abidor Complaint, *supra* note 4, at 1.

> the 3.7 million travelers referred to secondary inspection.[164]

Is that right? Only 0.018 percent of travelers had their laptops searched? That doesn't seem like much of a problem.

Upon examination, Abidor's numbers and the DHS numbers are not inconsistent with each other. According to Abidor's figures, over twenty months, 6500 electronic storage devices were searched; according to the DHS figures, over seven months, 2272 electronic storage devices were searched. Using some simple math, Abidor's figures result in 325 searches per month and the DHS figures reflect 324.6 searches per month—out of the approximate 530,000[165] travelers referred to secondary searches each month.

Obviously, the figures reflect a sufficient enough number of searches that privacy advocates are concerned—but will the courts pay attention? Are the numbers so low that courts might overlook the potential problem due to broader concerns about national security interests?[166] The fact that DHS is keeping track of the searches might be enough to minimize the concern that the privacy rights of individuals are being affected. Maybe Abidor's situation is unique—the figures suggest that the average American is not likely to have any problems with border searches of electronic devices.

F. Impact of Encryption

Should customs agents seize an electronic device if they cannot read the data in it? If they do seize it, how long can they keep it in an effort to uncover the data? Seemingly, it does little good for CBP or ICE to seize an electronic device if they cannot do anything with it. Assuming they do seize it, how long can they reasonably hold and examine the device? Does the mere fact that

---

[164] DEPARTMENT OF HOMELAND SECURITY PRIVACY OFFICE, ANNUAL REPORT TO CONGRESS JULY 2009–JUNE 2010 at 49 (2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf (emphasis added).

[165] This figure was obtained by doubling the DHS figure of 3.7 million travelers referred to secondary searches over a six-month period of time, and then dividing that figure by twelve months.

[166] *See supra* notes 126-27 and accompanying text (reflecting on Justice Kennedy and the potential for overlooking a small problem to prevent a much larger problem).

the agents detect that the device possesses encrypted data give agents reasonable suspicion that crime is afoot, thus mooting any concerns about potential Fourth Amendment violations?

"[E]ncryption is the process of transforming information . . . using an algorithm . . . to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key."[167] Given the pressing demands at the border, the average CBP or ICE agent is not likely to possess that "special knowledge." Are agents likely to see electronic devices utilizing encryption as a means to protect the privacy of data?

Will travelers use programs like TrueCrypt—"Free open-source on-the-fly encryption"[168]—freely available to anyone interested in using it? Truecrypt.org even offers "step-by-step instructions on how to create, mount, and use a TrueCrypt volume"[169]—so even beginners can use their product.

Assuming a traveler uses encryption and law enforcement wants to be able examine the electronic data of the traveler, will law enforcement be able to crack it? Will the law enforcement officer examining the electronic device even be able to know that an encrypted partition of the hard drive exists? Assuming the following comments to be accurate, encryption presents agents with a serious problem. Not only is it likely that agents won't be able to access the data, they might not even be able to know that the data is encrypted:

> The FBI has admitted defeat in attempts to break the open source encryption used to secure hard drives seized by Brazilian police during a 2008 investigation. . . . Brazilian reports state that two programs were used to encrypt the drives, one of which was the popular and widely-used free open source program TrueCrypt. Experts in both countries apparently spent months trying to discover the passphrases using a dictionary attack, a technique that involves trying out large numbers of possible character

---

[167] *StorageCraft Knowledge Base: Encryption*, STORAGECRAFT http://www.storagecraft.com/kb/glossary.php?letter=E (last visited Jan. 24, 2012); *see also Definition: Encryption*, SEARCHSECURITY.COM, http://searchsecurity.techtarget.com/definition/encryption (last visited Jan. 24, 2012).

[168] TRUECRYPT, http://www.truecrypt.org/ (last visited Jan. 24, 2012).

[169] *Beginner's Tutorial*, TRUECRYPT.ORG, http://www.truecrypt.org/docs/?s=tutorial (last visited Jan. 24, 2012).

> combinations until the correct sequence is found. Brazilian reports mention that the authorities had no means of compelling the makers of TrueCrypt to help them though it is hard to see how its creators could have helped. If a complex passphrase has been used – a random mixture of upper and lower case letters with numbers and special ASCII characters throw in – and the bit length is long, formidable computing power and time would be required to chance upon the correct passphrase. TrueCrypt also uses what is termed a "deniable file system" approach to encrypting whole hard drives. *Under this design, the existence of the encrypted partition will not be obvious to anyone examining the drive[,] allowing the individual using such encryption to plausibly deny its existence.*[170]

If the criminal transports his illicit data on electronic devices at the border[171] and uses some kind of encryption, it seems possible that the CBP agents might not even be able to recognize that the data is encrypted. If the CBP agents do recognize that encryption is in place, what should they do?[172] How long can they

---

[170] John E. Dunn, *FBI hackers fail to crack TrueCrypt,* TECHWORLD.COM, (June 30, 2010 10:55 AM), http://news.techworld.com/security/3228701/fbi-hackers-fail-to-crack-truecrypt/ (emphasis added).

[171] Who is likely to transport their illegal items on electronic devices at the border? Will the really bad guys—the terrorists—do it this way? There are certainly more private (i.e., not exposed to CBP agents) electronic methods for transferring electronic data from one place to another. Tech-savvy criminals will likely use another method. If that is accurate, it seems like the CBP and ICE policies regarding searches of electronic data will only catch the non-tech-savvy criminals and those so attached to their illicit data—like child pornography collectors—that they don't want to give up possession of it. *See* KENNETH V. LANNING, NAT'L CTR. FOR MISSING AND EXPLOITED CHILDREN, CHILD MOLESTERS: A BEHAVIORAL ANALYSIS—FOR PROFESSIONALS INVESTIGATING THE SEXUAL EXPLOITATION OF CHILDREN 91 (5th ed. 2010), *available at* http://www.missingkids.com/en_US/publications/NC70.pdf ("No matter how much the preferential sex offender has, he never seems to have enough. He rarely throws anything away. If law enforcement has evidence an offender had a collection 5 or 10 years ago, chances are he still has the collection now – only it is larger."). Beyond that kind of criminal, who is left that the policies might impact? Only the average U.S. citizen?

[172] Can they force the possessor to give up passwords? While a detailed discussion of this subject is beyond the scope of this Article, the answer appears to likely be no, due to the Fifth Amendment privilege against self-incrimination—assuming giving up the password is deemed "evidence of a testimonial or communicative nature." Schmerber v. California, 384 U.S. 757, 761 (1966) ("We hold that the privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State

hold the electronic devices for further examination? Encryption does not leave the agents in a good place. It appears that when TrueCrypt is used on a laptop, it would be nearly impossible to either break into the laptop or to detect it on a user's hard drive at currently available technological standards.

Does the fact that encryption exists as an alternative for criminals suggest that it will be reasonable for CBP agents to hold the laptops for longer periods of time?[173] The fact that CBP agents detect an encrypted volume on a laptop might add to the reasonable suspicion to justify the continued detention of the laptop. But what is this reasonable suspicion of? What "crime" is afoot?

If use of encryption becomes widespread, it may lessen the relevancy of any court ruling regarding border searches. The "smart" criminals will find another way to get their illegal data

---

with evidence of a testimonial or communicative nature, and that the withdrawal of blood and use of the analysis in question in this case did not involve compulsion to these ends." (footnote omitted)); *see* United States v. Kirschner, No. 09-MC-50872, 2010 WL 1257355, at *3 (E.D. Mich. Mar. 30, 2010) (forcing surrender of password violated Fifth Amendment); *In re* Boucher, No. 2:06-MJ-91, 2009 WL 424718, at *3-4 (D. Vt. Feb. 19, 2009) (finding no Fifth Amendment violation in later requiring a defendant to provide the password for an encrypted drive when the defendant had previously, post-Miranda warnings, voluntarily showed agents the encrypted drive on a laptop where child pornography was observed); *see also* John Duong, *The Intersection of the Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border*, 2 DREXEL. L. REV. 313 (Fall 2009) (discussing *In re Boucher*, 2009 WL 424718); Susan Brenner, *Passwords and the 5th Amendment Privilege*, CYB3RCRIM3 BLOG (April 28, 2010 7:58 AM), http://cyb3rcrim3.blogspot.com/2010/04/passwords-and-5th-amendment-privilege.html.

[173] In the context of criminal search warrants for electronically stored information, Federal Rule of Criminal Procedure 41(e)(2)(B) states: "Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Notably, due to "encryption" and other concerns, no time limit was set for later searches of electronic devices. *See* FED. R. CRIM. P. 41 advisory committee's note (2009) ("While consideration was given to a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place, the practical reality is that there is no basis for a "one size fits all" presumptive period. A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs. The rule does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the warrant is issued. However, to arbitrarily set a presumptive time period for the return could result in frequent petitions to the court for additional time.").

into the United States. That might motivate the Court to simply leave the existing—suspicionless—measures in place. At least that way, CBP agents will capture the less tech-savvy criminals and it might also make the other criminals work harder to avoid detection—in the process, they might still catch a few of the "smart" ones too.

V. GENERAL REFLECTIONS

What would the Court say if the *Abidor* case, or a similar case, found its way to the Supreme Court? Given the trepidation voiced in *Quon*, the Court is not likely to go out on a limb about technology. Any decision they make would probably be decided narrowly and be consistent with the pro-government approach to border searches that the Court has exhibited in the past.[174]

If compelled from the facts of the case to rule, the Court would likely conclude, consistent with the majority of lower courts, the initial seizure and search of an electronic device is routine and no reasonable suspicion is required. The search of an electronic device is not similar to a body cavity or strip search requiring individualized suspicion; an electronic device is more like property (like the gas tank in *Flores-Montano*) and can be searched without suspicion. The search of an electronic device is not distinctly "offensive"—thus closing the window left open in *Flores-Montano* for situations that might require individualized suspicion. The typical search of an electronic device at the border would not be deemed so "destructive" as to require a different result.[175] Quite simply, an electronic device, despite the fact that it can contain vast amounts of personal information, is not an extension of the body—it is property like a piece of luggage. Additionally, as some lower courts have noted,[176] the search of an electronic device is no more offensive or destructive than a detailed search of any other

---

[174] The Court might simply deny any petition for a writ of certiorari as was done in the *Arnold* case. United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008), *cert. denied*, 129 S. Ct. 1312 (2009).

[175] And at least at the border, convergence of the Fourth Amendment with the First Amendment will not heighten the suspicion requirement. The *Ickes* court said it best in noting that to rule otherwise would result in an administrative nightmare at the border and would create a "sanctuary" for terrorists. United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005).

[176] *See supra* notes 79-85 and accompanying text.

property. The initial seizure and search of an electronic device will be looked at as little more than searching a piece of luggage that contains private information—an act that can be done by CBP and ICE agents without any suspicion at all.

Why? The role of "governmental interest" is affecting the interpretation of what is "reasonable" under the Fourth Amendment. The task of a CBP agent can be daunting. The mere flow of traffic—both in cars and people—seems too heavy to require, at least immediately at the border, any kind of individualized suspicion. Requiring the presence of individualized suspicion for the initial seizure and search of electronic devices at the border would significantly lessen or eliminate the deterrent effect that the present border search policy has on criminals in bringing contraband into the United States.

Most importantly, any decision the Court would make would likely be guided by the twenty-first century's biggest national security concern—the prevention of terrorism within our country. Consider the following statement made thirteen days after September 11, 2001:

> Anyone worried about the fate of civil liberties during the U.S. government's growing war on terrorism might want to consider this Latin maxim: Inter arma silent leges. It means, "In time of war the laws are silent," and it encapsulates the supremacy of security over liberty that typically accompanies national emergencies.[177]

Are we still facing a "national emergency"? Consider the words of Janet Napolitano, secretary of DHS, nearly ten years after September 11, 2001, in addressing the House Homeland Security Committee: "In some ways, the threat today may be at its most heightened state since the attacks nearly 10 years ago."[178] Ten years have passed and the only thing that seems to have changed is an increased intrusion on personal privacy—mostly in response to the fear of terrorism that does not seem to be going

---

[177] Declan McCullagh, *Why Liberty Suffers in Wartime,* WIRED.COM (Sept. 24, 2001), http://www.wired.com/politics/law/news/2001/09/47051.

[178] Eric Schmitt, *Lawmakers Hear of Threat by Domestic Terrorists*, N.Y. TIMES (Feb. 10, 2011), at A14, http://www.nytimes.com/2011/02/10/us/politics/10terror.html?ref=politics.

away. As the sophistication of terrorist tactics increases,[179] this intrusion on personal privacy will only get worse. This national security concern will most certainly impact any court's consideration of border searches of electronic devices.[180]

Is there no hope for Mr. Abidor or others like him? The time involved in retaining an electronic device for subsequent "off-site" search purposes may motivate the courts to find that reasonable suspicion of criminal evidence be present at some point. The ready availability of encryption increases the likelihood that agents will hold electronic devices for long periods of time. While in the context of a criminal case, the Court in *Place* clearly seemed troubled with law enforcement holding personal items for too long without any individualized suspicion.[181] Depending on the period of time involved, the Court might be compelled to hold that some level of individualized suspicion is necessary to hold an electronic device for further examination purposes.[182]

Assuming the Court requires reasonable suspicion of criminal activity in order to hold and examine a device beyond a particular period of time, is it going to be a tough standard for CBP and ICE agents to meet? Not likely. Time and again, the lower courts have found it unnecessary to examine the issue of whether individualized suspicion is needed because the evidence showed that reasonable suspicion was present.[183] Even if it is required,

---

[179] *See, e.g.*, Scott Shane & Robert F. Worth, *Earlier Flights May Have Been Dry Run for Plotters*, N.Y. TIMES, Nov. 1, 2010, at A14, *available at* http://www.ndtv.com/article/world/earlier-flight-may-have-been-dry-run-for-plotters-63959twrhp ("New details about the two explosive packages were disclosed by security officials in several countries, who discussed the continuing investigation on condition of anonymity. The explosive powder, pentaerythritol tetranitrate, or PETN, was found inside toner cartridges that were themselves inside HP LaserJet P2055 printers, according to officials from Germany and the United Arab Emirates.").

[180] Who will be affected if the Court allows the initial seizure and search to continue without any individualized suspicion? Certainly the child pornography possessors, since they seem to be the ones getting caught. *See supra* note 27 and accompanying text. Beyond that, the DHS statistical data seems to suggest that only a small portion of the remaining public will be affected. *See supra* note 164 and accompanying text.

[181] *See supra* notes 91-103 and accompanying text.

[182] *See supra* notes 33-65 and accompanying text (covering lower courts' discussion of the reasonableness of holding electronic devices for extended periods).

[183] *See supra* note 29 and accompanying text.

the Court has made clear that reasonable suspicion is not a hard standard for law enforcement to meet.[184]

CONCLUSION

Where will the Court draw the electronic line at the international border? Consider the following from *United States v. Thirty-Seven Photographs*:

> But a port of entry is not a traveler's home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search. Customs officials characteristically inspect luggage and their power to do so is an old practice and is intimately associated with excluding illegal articles from this country.[185]

It appears that the "firm line" remains at the home, not with the power button for electronic devices at the border.

Pascal Abidor's tribulations certainly make a compelling story. As the American public hears about this search of electronic devices at the border, and others like it, they will certainly sympathize with seemingly innocent participants like Abidor. While the Court has periodically observed that what is "reasonable"—and their opinion of what is "reasonable"—can be affected by social customs and public beliefs,[186] this is not one of

---

[184] *See, e.g.*, United States v. Arvizu, 534 U.S. 266, 277 (2002) (holding there was reasonable suspicion present when border patrol agent observed minivan with kids set out on a "little-traveled route used by smugglers," there was a much more efficient way to travel to their alleged recreational location, the "children's elevated knees suggested the existence of concealed cargo in the passenger compartment," and the agent's assessment of the defendant's "reactions upon seeing him and the children's mechanical-like waving, which continued for a full four to five minutes"); Illinois v. Wardlow, 528 U.S. 119, 124 (2000) (finding reasonable suspicion present, which justified stop of an individual in "an area known for heavy narcotics trafficking" who exhibited "nervous, evasive behavior" and engaged in "unprovoked flight upon noticing the police"); *see also supra* notes 124-25 and accompanying text (covering comments of Justice Scalia in *Flores-Montano* oral argument and suggesting that one should rely on the intuition of agents).

[185] United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971).

[186] *See, e.g.*, Georgia v. Randolph, 547 U.S. 103, 114 (2006) ("Since the co-tenant wishing to open the door to a third party has no recognized authority in law or social practice to prevail over a present and objecting co-tenant, his disputed invitation,

those examples. The concern for keeping our borders and our country's interior safe from terrorists and other criminals, combined with lower court and Supreme Court precedent, could prevent Abidor from ever obtaining effective and meaningful relief or leaving a lasting impression in the field of Fourth Amendment jurisprudence. Relief, if any, is likely to come from Congress.

In the meantime, CBP and ICE will continue to periodically turn on and look over laptops and other electronic devices without any suspicion at all. If encryption motivates the agents to retain the electronic devices for extended periods, courts might find that reasonable suspicion of criminal activity is present—but any such reasonable suspicion requirement won't be too hard to meet for the well-trained CBP agent.

People will adjust. Sophisticated criminals will encrypt more or send the data or contraband in other ways, the average citizen will transport less across international borders, and the child pornography possessors will continue to get caught because they just do not want to let go of their collection. Technology will not change how the robust Fourth Amendment applies to border searches, but it will impact how people behave at the border.

---

without more, gives a police officer no better claim to reasonableness in entering than the officer would have in the absence of any consent at all.").