Electronic Data at the Border

Safeguarding the Privacy of Our Thoughts

By Steven Torem
St. John's University School of Law
Class of 2010

85-28 212th Steet
Hollis Hills, NY 11427
(917) 468-0533
Submitted on May 17, 2010

Electronic Data at the Border: Safeguarding the Privacy of Our Thoughts

By Steven Torem

Introduction

Long lines, delays, invasive body scanning, underwear bombers – travelers entering and returning to the United States from abroad have no shortage of worries to accompany them on their trip. Now, individuals entering the United States from abroad carry with them a new source of complication – their own laptop computers and electronic devices. Most international travelers do not give a second thought to packing these items and using them to stay entertained, connected and productive while overseas. However, few consider that the vast amounts of personal information contained within a small hard drive, flash drive or memory card can be reviewed, downloaded and even copied by federal officers tasked with securing our nation's borders. Recently, these searches have been upheld under the border search exception to the fourth amendment. But does this exception for routine border searches rightfully cover in depth searches of electronic data?

There are 327 official ports of entry into the United States, each one a potential open door for individuals carrying out, or planning crimes such as drug trafficking, child pornography and terrorism.[1] These ports of entry include the northern and southern border crossings, airports, seaports, lakes, rivers and coastlines – and wherever an official port exists, the U.S. Department of Homeland Security ("DHS") is tasked with securing and facilitating trade and travel through that port.[2] To help accomplish this mission, the Department of Homeland Security, which

[1] U.S. Customs and Border Patrol, http://www.cbp.gov/xp/cgov/toolbox/ports/ (last visited April 1, 2010).
[2] *See Id.*

includes the agents of Customs and Border Patrol ("CBP"), works within the broad framework of the so-called border search exception to the Fourth Amendment.[3]

The border search exception permits law enforcement officers to conduct routine searches of persons or objects entering, and in some cases exiting[4] the United States, without a warrant and without demonstration of any level of suspicion.[5] The Supreme Court has justified this broad power by recognizing the nation's inherent sovereign authority to protect its territorial integrity at the border,[6] but courts continue to explore the scope of the exception. Specifically, at issue is the definition of a "routine search" in the context of the border search exception and whether or not the search of electronic data can be conducted without a warrant and without suspicion.

I. The Fourth Amendment and the Border Search Exception

The Fourth Amendment to the United States Constitution regulates searches and seizures carried out by government officials.[7] In general, this Amendment has been interpreted by the Supreme Court to require, prior to conducting a search, that police officers and other government officials must obtain a warrant from a neutral magistrate that particularly describes the person, place, or items to be searched.[8] Searches carried out without a warrant are "per se unreasonable" subject only to a handful of specifically established and well delineated exceptions.[9] Regardless

[3] U.S. CONST. amend. IV
[4] See generally Larry Cunningham, The Border Search Exception as Applied to Exit and Export Searches: A Global Conceptualization, 26 Quinnipiac L. Rev. 1 (2007).
[5] In the context of our nation's borders, courts have carved out an exception to the fourth amendment such that no degree of probable cause is necessary to search the contents of a traveler's person and luggage. *United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985)*.
[6] *United States v. Flores-Montano*, 541 U.S. 149, 151 (2004)
[7] U.S. Const. amend. IV. This amendment provides "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures," and that "no Warrants shall issue, but upon probable cause."
[8] *Id.*; see also *Kyllo v. United States*, 533 U.S. 27 (2001)
[9] *Katz v. United States*, 389 U.S. 347, 357 (1967)

of the exception, in almost every situation, government officials must still demonstrate some degree of suspicion prior to the search "indicating that the individual is about to, has already, or is in the process of committing a crime."[10]

For example, when government officials conduct searches of vehicles and containers, courts have recognized the need to excuse the warrant requirement. However, that officer must be able to show that prior to the search, he had probable cause to believe that evidence of the crime, or a weapon, would be found inside the vehicle or container.[11] Likewise, no warrant is required for brief, non-intrusive searches of a person for weapons (stop and frisks) where an officer has a reasonable suspicion that the individual poses a danger to his safety or the safety of the public.[12] Reasonable suspicion is a lower standard than probable cause, and it is all that is required for a brief stop and frisk-style search.[13]

Courts have deviated from these standards when searches are particularly intrusive or when the government's need is particularly great. When a search is unusually intrusive, such as a blood test, courts typically require a higher degree of probable cause.[14] More often than not, courts tend to relax the probable cause and reasonable suspicion standards when the government demonstrates a convincing need to do so. Such is the case in public schools where school employees, who are undeniably government actors, are permitted to conduct searches of a student's belongings without any showing of probable cause.[15]

---

[10] Coletta, Christine A., 48 B.C. L. Rev. 971, 977 (2007)
[11] *California v. Acevedo*, 500 U.S. 565 (1991) (allowing warrantless search of a container with probable cause); *Chambers v. Maroney*, 399 U.S. 42 (1970) (probable cause required for warrantless search of vehicle); *Carroll v. United States*, 267 U.S. 132 (1925) (same).
[12] *Terry v. Ohio*, 392 U.S. 1 (1968)
[13] *Id.* at 27-31.
[14] See *Schmerber v. California*, 384 U.S. 757, 769 (1966) (where court required a clear indication that incriminating evidence would be found before it allowed blood to be drawn).
[15] *New Jersey v. T.L.O.*, 469 U.S. 325 (1985) (Searches permitted without probable cause because of need to ensure school safety and unique problem of keeping drugs off of school grounds)

Another context in which courts have given the government broad authority to conduct searches is at the nation's borders. The border search exception is unique in that its justification is not based on exigency or the impracticability of obtaining a warrant, but on the recognized right of the sovereign to control who and what may enter the country.[16] Although travelers still have some expectation of privacy, the government's need to secure the borders outweighs and even minimizes this individual right to privacy.[17] Because of this recognized right of the sovereign and the importance of protecting the borders, routine searches of an international traveler's belongings and person can be performed without a warrant and without any degree of suspicion.[18] Searches of a non-routine nature, however, require reasonable suspicion,[19] but instances of courts characterizing a search as non-routine are limited.

II. Evolution of the Border Search Exception

A. Early Cases

The border search exception was first officially recognized by the Supreme Court in 1977,[20] though it was alluded to in prior case law and early legislation. In *Boyd v. United States*,[21] the Supreme Court upheld the seizure of illegally imported goods under the Fourth Amendment, citing common law and an act of the First Congress authorizing border searches and seizures without probable cause.[22]

---

[16] *Ramsey v. United States*, 431 U.S. 606, 620 (1977).
[17] *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004); see *Ramsey*, 431 U.S. at 624 (1977); *United States v. Uribe-Galindo*, 990 F.2d 522, 526 (10th Cir. 1993).
[18] For routine searches, customs officials may search travelers and their luggage without a warrant and without probable cause. *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). "Routine searches include those searches of outer clothes, luggage, a purse, wallet, pockets, or shoes, which unlike strip searches, do not substantially infringe on a traveler's privacy rights." *United States v. Irving*, 452 F.3d 110, 123 (2nd Cir. 2006)
[19] *United States v. Humphries*, 308 Fed. Appx. 892, 896 (6th Cir. 2009).
[20] *United States v. Ramsey*, 431 U.S. 606, 619 (1977).
[21] *Boyd v. United States*, 116 U.S. 616, 617 (1886).
[22] When the First Congress convened, it passed a customs statute that exempted border searches from probable cause and warrant requirements. Act of July 31, 1789, ch. 5, § 24, 1 Stat. 29, 43 ("That every collector, naval officer, and surveyor, or other person specially appointed by either of them for that purpose, shall have full power and authority, to enter any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to

This power was reaffirmed by the Supreme Court in *United States v. Ramsey*, when the Court directly addressed the constitutionality of warrantless and suspicionless border searches.[23] The defendants in *Ramsey* were convicted of, among other things, possession of narcotics and illegal importation of heroin. These individuals ran a heroin-by-mail enterprise in which drugs from Thailand would be sent, by international mail, to the United States for distribution. Key evidence against the defendants was obtained when a customs officer at the sorting facility of the New York Post Office noticed several bulky envelopes all originating from Thailand. After determining that the envelopes contained something other than letters, the customs officer then opened the envelopes and discovered the narcotics. Addressing the constitutionality of this warrantless border search, the Court held that such searches were permissible because of the diminished expectation of privacy at the border.[24] As it did in *Boyd*, the Court based its holding on authority predating the Fourth Amendment, writing: "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 has entered into our country from outside*."[25] This passage reflects the special significance of the border in the eyes of the Court.

Subsequently, the Court echoed this reasoning in *United States v. Montoya de Hernandez,*[26] noting that, "since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."[27] The Court in *Montoya de Hernandez* held that

---

duty shall be concealed; and therein to search for, seize and secure any much goods, wares or merchandise…"). See also Cunningham, *supra* note 4, at 4.

[23] *Ramsey*, 431 U.S. 606 (1977) .

[24] *Id.* at 623, n.17.

[25] Cunningham, *supra* note 4, at 10 (quoting Ramsey, 431 U.S. at 619).

[26] *Montoya de Hernandez*, 473 U.S. 531 (1985)

[27] *Id.* at 537 (citing Ramsey, 431 U.S. at 616-17)

reasonable suspicion is not required for random searches of any incoming international passenger and that customs officials may search travelers and their luggage without a warrant or probable cause.[28] In the last several decades, the scope and reach of the exception has been further clarified and expanded through this and other judicial decisions.

B. Physical Reach of the Border Search Exception

Despite its name, a border search need not take place at an actual border.[29] The same rationale that supports the application of the border search exception at traditional ports of entry also applies to international airports and other functional equivalents of the border.[30] This may include areas immediately surrounding the border where it is anticipated that individuals in the vicinity will be making an imminent border crossing.[31]

In some circuits, the border search exception has even been used to justify a so-called "extended border search" which can occur a great distance away from the actual border – for example, at regional package sorting facilities receiving and delivering international parcels.[32] This extension of the border search exception allows for the application of a lower reasonable suspicion standard, rather than the standard probable cause or warrant requirements that would normally apply in such locations.

C. Development of Routine/Non-Routine Distinction

Despite the broad authority conferred by the border search exception, the Court has acknowledged that there are some constitutional limits on the doctrine. Although there is no

---

[28] *Id.*
[29] *United States v. Abbouchi*, 502 F.3d 850, 855 (9th Cir. 2007)
[30] *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973); *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. N.Y. 2006); *United States v. Gaviria*, 805 F.2d 1108, 1112 (2d Cir. 1986) (airport serving as final destination for nonstop international flight deemed functional equivalent of border).
[31] *See Humphries*, 308 Fed. Appx. 892 (6th Cir. 2009).
[32] *Abbouchi*, 502 F.3d 850, 855 (9th Cir. 2007) (holding that the search of an international package at a UPS sorting facility qualified as a border search because it represented the last practical opportunity to perform a search prior to the parcel's departure from the US); *United States v. Seljan*, 547 F.3d 993 (9th Cir. 2008).

bright-line rule,[33] highly intrusive searches, such as body cavity, strip and x-ray searches have all been considered non-routine and thus subject to constitutional limitation.[34]

In *United States v. Montoya de Hernandez*,[35] the defendant, Rosa Elvira Montoya de Hernandez, was selected for further questioning after she arrived at Los Angeles International Airport on a flight from Bogota, Colombia. A customs inspector grew suspicious because the defendant had made several recent trips to Miami and Los Angeles, had no friends in the United States, did not have a hotel reservation, had $5000 in cash but no billfold, could not recall how she purchased her plane ticket, and had a suspicious story about coming to the United States to buy supplies for her husband's store. After these suspicious responses to the initial line of questioning, customs inspectors performed a pat-down of the defendant which revealed that her abdomen felt firm and full. As a result of these findings, the inspectors accused the defendant of being a "balloon swallower," one who attempts to smuggle narcotics hidden in the alimentary canal. After withdrawing her consent to an x-ray of her stomach, the defendant was detained for 16 hours until a court order authorizing an x-ray and rectal exam was secured. At the hospital, doctors eventually removed nearly 100 small balloons containing a total of 528 grams of cocaine.[36]

The issue before the Court in *Montoya de Hernandez* was the constitutionality of the sixteen hour detention and seizure of the defendant. Citing the government's broad power to perform searches and seizures at the border, the majority noted the government's concern over the ever increasing drug smuggling industry, and in particular the use of alimentary canal

[33] See *Flores-Montano*, 541 U.S. at 152.
[34] *Montoya de Hernandez*, 473 U.S. at 541.
[35] *Id.*
[36] *Id.* at 532-36.

smuggling.[37] Because the government's interests in protecting the border are so strong, the "Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior."[38] The defendant voluntarily requested admission to the country and subjected herself to the laws of the United States, therefore her expectation of privacy at the border was lessened.[39] In this case, the Court balanced privacy against the government's interest at the border – and the government won.[40]

Although the Court admitted that individualized suspicion was unnecessary in the case of a routine border search, the Court found that the dignity and privacy interests implicated in the search and detention of Ms. Montoya de Hernandez elevated the procedure "beyond the scope of a routine customs search and inspection…"[41] For the first time, the Court had to decide what level of suspicion, if any, was required for a non-routine search or seizure at the border.[42] Rejecting the Ninth Circuit's "clear indication" test, the Supreme Court held that "reasonable suspicion" was required for the non-routine border search of the defendant's alimentary canal.[43] The Court therefore upheld the search and detention at issue in the case because the inspectors had reasonable suspicion to believe that the defendant had drugs in her alimentary canal.[44]

Similarly, the Court has suggested that border searches carried out in a particularly offensive manner may also be consider non-routine.[45] A border search might be particularly offensive if, irrespective of dignity or privacy interests, it is highly intrusive or destructive of

[37] *Montoya de Hernandez*, 473 U.S. at 537-38.
[38] Cunningham, *supra* note 4, at 13 (quoting *Montoya de Hernandez*, 473 U.S. at 538).
[39] *Montoya de Hernandez*, 473 U.S. at 539 (citing *Carroll v. United States*, 267 U.S. 132 (1925); 19 U.S.C. § 482 (1982)).
[40] *Id.* at 540.
[41] *Id.* at 541.
[42] *Id.* at 540.
[43] *Id.* at 541.
[44] *Id.*
[45] *Flores-Montano*, 541 U.S. at 155, n.2.

personal property.[46] However, the Court has limited the usefulness of this exception to the exception by imposing a high burden. For example, in one prior case, the Court found that a search that took about an hour and required the disassembly and reassembly of a vehicle's gas tank was, in fact, an ordinary, routine border search that did not require individualized suspicion.[47]

D. Courts Begin to Question Where Laptops Fit

United States v. Ickes

It is with this historical background that the courts have had to analyze the modern issue of laptop searches at the border. Before recently, courts have avoided deciding the standard of suspicion necessary to search or seize laptops and other electronic data by declining to categorize these items as routine or non-routine. In *United States v. Ickes*,[48] the Fourth Circuit affirmed a lower court's denial of a motion to suppress evidence of child pornography found during a border search.[49] Ickes was stopped while attempting to enter the United States from Canada, at a port of entry near Detroit. A customs inspector became suspicious because Ickes claimed he was returning from vacation but his van appeared to contain all of his belongings. At that point, Ickes was referred to a secondary inspection station where another customs agent discovered a video camera containing footage of a tennis match that seemed to focus excessively on a young ball boy. This discovery prompted a thorough search of the van which turned up marijuana, marijuana pipes, a copy of a Virginia warrant for Ickes' arrest, and several albums containing photographs of nude and semi-nude prepubescent boys.[50] The agents then arrested Ickes and continued the search of his van which produced a computer and approximately 75 disks

[46] *Id.* at 155-156.
[47] *Id.*
[48] 393 F.3d 501 (4th Cir. 2004).
[49] *Id.* at 502.
[50] *Id.* at 503.

containing additional child pornography, including a home movie of Ickes engaged in sexual acts with two minor children.[51]

At issue in the case was the constitutionality of the laptop border search. Ickes argued that the court should recognize a First Amendment exception to the border search doctrine, claiming that the border search exception did not apply to "expressive material," and that the lower court's ruling was overly sweeping[52] and beyond the scope of Congress' authorization in 19 US.C. § 1581.[53]

The Fourth Circuit rejected both of these arguments. First, the court affirmed the customs agents' broad statutory authority to search the defendant's van and computer at the border.[54] Citing the expansive language of the statute, the court determined that a laptop computer was within the category of items that a customs official may properly search.[55]

Next, the court considered whether, notwithstanding the statutory authority, a border search of a laptop computer is constitutional.[56] To do so, the court employed a two step balancing approach to determine whether the search required individualized suspicion and whether the search was reasonable.[57] It affirmed that probable cause was not required for customs agents to search the defendant's computer but declined to decide what level of suspicion, if any, would be needed for similar searches in the future.[58] Instead, the court concluded that this

---

[51] *Id.*
[52] *Id.*
[53] 19 U.S.C. § 1581(a) (2000). This statute contains an emphatic empowerment of U.S. Customs officials: "Any officer of the customs may at any time go on board of any vessel of vehicle at any place in the United States or within the customs waters, …or at any other authorized place…and examine the manifest and other documents and papers and examine, inspect and search the vessel or vehicle and every part thereof any any person, trunk, package, or cargo on board.."
[54] *Ickes*, 393 F.3d. at 504.
[55] *Id.* (Writing "[w]e are unpersuaded that these particular transported goods are somehow exempt from the ordinary definition of cargo.")
[56] *Id.* at 505.
[57] *Id.* at 507; *see New Jersey v. T.L.O.*, 469 U.S. 325, 341 (suggesting a two-step analysis to determine the reasonableness of warrantless searches).
[58] *Id.*

issue was moot since the agents had reasonable suspicion to validate the search.[59] Finally, the court balanced the interests of the government against the individuals privacy rights and found, as the Supreme Court had previously in *United States v. Montoya de Hernandez* and *United States v. Ramsey,*[60] that at the border, the balance favors the government's interest as sovereign.[61]

In refusing to carve out a First Amendment exception to the border search doctrine, the court expressed its worry that such an exception would "create a sanctuary at the border for all expressive material – even for terrorist plans."[62] In fact, the Fourth Circuit noted that cases such as *Ramsey,* contrary to the defendant's assertion, indicated a reluctance to accord greater protection for expressive material.[63] Ickes failed to make a Fourth Amendment argument in this case, but the court did caution that border searches must comport with the reasonableness requirement of the amendment. The court noted that this reasonableness requirement was met "in light of the Supreme Court's recent instruction that searches of belongings at the border `are reasonable simply by virtue of the fact that they occur at the border.'"[64]

United States v. Romm

Two years after *Ickes*, in *United States v. Romm,*[65] the U.S. Court of Appeals for the Ninth Circuit held that a customs official does not need reasonable suspicion to search a laptop computer at a U.S. border.[66] En route to a business training seminar in Canada, Romm was stopped by agents of the Canada Border Services Agency for questioning after a routine check

[59] *Id.* As proof of suspicion, the court noted the many factors that led up to the search of the defendant's van, including the suspicious responses made to questioning, the drug paraphernalia and the warrants for Ickes' arrest.
[60] *Ramsey*, 431 U.S. 606 (1977).
[61] *Ickes*, 393 F.3d. at 506; see *Montoya de Hernandez*, 473 U.S. at 540; *Ramsey*, 431 U.S. at 619.
[62] *Id.* at 506.
[63] *Id.* at 507.
[64] *Id.* at n.1 (quoting *Flores-Montano*, 541 U.S. at 152-53)
[65] *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006)
[66] *Id.* at 994.

showed that he had a positive criminal history. While being questioned, one Canadian agent searched Romm's computer and discovered several child pornography websites in his browser history. Canada denied him entry to the country and Romm returned to the U.S. on a flight to Seattle. At the Seattle-Tacoma airport, Romm was interviewed by U.S. Customs officials who informed him that they needed to search his laptop. Romm consented to the search and a forensic analysis of the hard drive was performed. On his hard drive, agents found evidence of ten child pornography pictures that had been previously deleted from his computer's memory.[67]

On appeal, Romm argued that the search of his laptop was too intrusive on his First Amendment rights to qualify as a routine border search.[68] The court repeated the Supreme Court's *Montoya de Hernandez* reasoning that routine searches at the border do not require reasonable suspicion.[69] However, the court stopped just short of classifying the laptop search as routine or non-routine. Unfortunately, since the issue was not raised until the defendant's reply brief, the court considered this defense waived.[70]

United States v. Arnold

In 2008, the Ninth Circuit once again considered the constitutionality of laptop searches in *United States v. Arnold*, finally deciding the issue of whether laptop searches are routine or non-routine.[71] The defendant, Michael Timothy Arnold, arrived at Los Angeles International Airport on a flight from the Philippines. After retrieving his luggage, Arnold proceeded to a customs checkpoint where he was selected for secondary questioning by a CBP agent. During questioning, customs agents searched Arnold's luggage and found a USB flash drive, six

[67] *Id.*
[68] *Id.* at 996.
[69] *Id.* (finding that customs officials must be granted a great deal of discretion to conduct suspicionless border searches).
[70] *Id.*
[71] 533 F.3d 1003.

compact disks, and a laptop computer which they instructed Arnold to boot up. As the computer turned on, it was handed off to a second customs agent while the luggage search continued. Once the computer had booted up, its desktop displayed numerous icons and folders, at least two of which appeared to contain photographs. The customs agents opened these folders and viewed the files contained therein. When agents found a photo depicting two nude women, they called in special agents with the US Department of Homeland Security, Immigration and Customs Enforcement ("ICE"). The ICE agents questioned Arnold and detained him for several hours. Ultimately, a detailed search of the computer and electronic storage devices revealed numerous images containing what appeared to be child pornography. Two weeks later, on the basis of the border search, federal agents were granted a warrant to search the computer and storage devices.[72]

The District Court for the Central District of California characterized the search of the laptop as *non-routine*, reasoning that the Fourth Amendment requires the government to possess reasonable suspicion to perform a search that implicates the privacy and dignity interests of a person.[73] This significant holding was the first to recognize the special nature of laptop computers and the first to clearly hold that laptop searches were non-routine.[74] The court held that the customs officials lacked reasonable suspicion and suppressed the evidence found in the border search as well as the subsequent search two weeks later.[75]

---

[72] *Id.* at 1005.
[73] United States v. Arnold, 454 F. Supp. 2d 999, 1000-01 (C.D. Cal. 2006).
[74] *Id.* "While not physically intrusive as in the case of a strip or body cavity search, the search of one's private and valuable 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." *Id.*
[75] *Id.* at 1001.

On appeal, this holding was reversed by the Ninth Circuit who declined to split with the Fourth Circuit's decision in *United States v. Ickes*.[76] Arnold argued that "laptop computers are fundamentally different from traditional closed containers,"[77] analogizing the hard drive of a laptop computer to a home because of its vast storage capacity, and to the human mind because of the computer's ability to record ideas, emails, Internet chats and web-surfing habits.[78] Disagreeing with Arnold's characterization of laptop computers, the court said that, laptops, akin to vehicles, are simply pieces of property that do not implicate the same dignity and privacy concerns as would highly intrusive searches of a person.[79] The court held that laptop searches are routine border searches and as such, they do not require a showing of reasonable suspicion.[80] The Supreme Court denied certiorari and the Ninth Circuit's holding has since been followed in subsequent cases.[81]

Read together, *Ickes* and *Arnold* seem to suggest that the government may search a laptop computer or any other electronic storage device at the border, for any legal reason or no reason at all.[82] The *Ickes* court legalized suspicionless border searches of electronic devices, and the *Arnold* court embraced and expanded these searches. Under *Arnold*, government officials at international check points may now require an individual to turn on their laptop computer and are then permitted to open any and all of the files contained therein without any individualized suspicion.

III. Criticism and Necessity of the Border Search Exception

[76] *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008).
[77] *Id.* at 1006.
[78] *Id.*
[79] *Id.* at 1008.
[80] *Id.* at 1010.
[81] *See United States v. Hilliard*, 289 Fed. Appx. 239 (9th Cir. 2008).
[82] Chacon, Jennifer, Border Searches of Electronic Data, 2008 Emerging Issues 2430 (June 30, 2008)

Most U.S. citizens would agree that the government has a duty to protect the nation from terrorist threats and to uphold our laws, however those same citizens would likely be surprised to learn that their computers, smart phones, USB drives, compact disks and external hard drives can all be searched, copied and archived whenever they travel overseas. Therein lies the inherent challenge in the border search exception – the balance of individual privacy interests and the government's interest in protecting the borders and enforcing U.S. law.

On September 11, 2001, our nation suffered the deadliest attack ever on U.S. soil. "More than 2,600 people died at the World Trade Center; 125 died at the Pentagon; 256 died on the four planes. The death toll surpassed that at Pearl Harbor in December 1941."[83] Zacarias Moussaoui, a member of the 9/11 conspiracy alleged to be a replacement hijacker, kept information on his laptop that, if discovered, might have prevented the unspeakable tragedy.[84] More recently, in 2006, a laptop search at Minneapolis-St. Paul International airport helped CBP identify a high-risk traveler. A search of this individuals laptop revealed video clips of roadside bombs being used to kill U.S. soldiers and destroy vehicles, as well as a video on martyrdom.[85]

Border searches of electronic data have also netted numerous arrests and convictions for other illegal activities. In fact, the vast majority of federal cases challenging the constitutionality of laptop border searches have dealt with the subject of child pornography. With its proven track record of disrupting terrorist plans and catching child pornographers, there is little doubt that border searches of electronic data can be a valuable tool for law enforcement and national

[83] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Page 1-2 (2004).
[84] Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary, 110th Cong. 4 (2008) (Statement of Hon. Sam Brownback, Senator from the State of Kansas).
[85] *Id.* at 8-9 (Staement of Nathan A. Sales, Assistant Professor of Law, George Mason University School of Law).

security. The question is whether this tool is being wielded correctly and responsibly in a way that comports with Fourth Amendment protections.

Laptop computers, smart phones, and other electronic storage devices have become increasingly entrenched in the lives of U.S. citizens. These devices have the potential to contain a vast amount of business, financial, and personal information, much of which can be sensitive in nature.[86] For example, just one cellular phone can contain audio and video files, photographs, contact information, and financial records; a USB drive no bigger than a pack of chewing gum can hold tens of thousands of documents; and the amount and scope of information that can be held within a laptop's memory is exponentially greater. Even more worrisome is the permanence of this data – electronic storage devices can be seized, and files can easily be copied, stored and archived indefinitely for later retrieval.[87] This is permitted by CBP protocol,[88] and has been carried out by officials during border searches.[89] Even data that has been erased can be recovered be trained forensic technicians or laypersons using a variety of off-the-shelf software and hardware solutions.[90]

---

[86] Customs and Border Patrol has recently published their internal guidelines which give specific guidance on the search of certain types of electronic information, namely Business Information, Sealed Letter Class Mail, and Attorney Client Privileged Information. All but Sealed Letter Class Mail may be opened and read, but CBP advises its officers to protect confidential business information from unauthorized disclosure, and to consult with the U.S. Attorney's Office before searching any attorney-client material that the officer suspects may contain evidence of a crime. U.S. Customs and Border Patrol, Policy Regarding Border Search of Information, http://cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf (July 16, 2008) (last visited April 10, 2010)

[87] *See Id.* CBP has published vague guidelines for the storage and retention of electronic information. Although clearly authorized to seize and copy electronic information, customs agents are instructed not to retain information if there is no probable cause of illegal activity generated from a review of the information. Absent probable cause, customs officials may still retain copies of electronic data that relate to immigration matters.

[88] U.S. Customs and Border Patrol, Policy Regarding Border Search of Information, http://cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf (July 16, 2008) (last visited April 10, 2010).

[89] *Id*. at 11 (Statement of Susan K. Gurley, Executive Director of the Association of Corporate Travel Executives); s*ee also Arnold*, 533 F.3d at 1005; Chacon, 2008 Emerging Issues 2430 at 3.

[90] *Id*. at 7 (Statement of Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation)(Recent technology makes forensic analysis of computers and other electronic storage devices possible even for untrained personnel. For example, Microsoft recently released a USB thumb drive that contains 150 automatic commands meant to dramatically cut the time it takes to gather digital evidence. Another device, known as the CSI stick, can capture all

The Association of Corporate Travel Executives ("ACTE") has stated that this seizure, copying and retention of sensitive information can impose a personal and financial burden on business travelers and their corporations.[91] In a survey of their members in February 2008, seven percent reported that they had been subject to the seizure of a laptop or other electronic storage device.[92] More alarmingly, 81 percent of respondents said that they were not even aware that the information contained on their electronic devices could be copied and held indefinitely during a border search.[93]

Electronic storage devices may contain highly sensitive trade secrets and correspondence. Journalists traveling on business might carry with them files containing the names of sources or drafts of work in progress. In response to these border search procedures, the ACTE reports that companies have been forced to implement new and expensive internal travel policies, including the use of web-accessible e-mail, file encryption, and investment in additional "scrubbed" laptops for travel use.[94]

The privacy concerns of the casual international traveler are no less numerous. No matter how personal electronic files may be, they are all subject to close inspection if one seeks to gain entry to, or exit from the country. In a statement concerning the border search of laptops and other electronic devices, even the former secretary of Homeland Security, Michael Chertoff, noted that "[t]here are absolutely privacy concerns."[95]

---

data on most models of cell phones including text messages, phone books, call logs, and multimedia messages ("MMS")); *see Romm*, 455 F.3d at 995 (Agents used software called "Encase" to recover deleted files, as well as information showing when the file was created, accessed and modified. Agents also recovered a list of websites visited by the defendant that remained on the hard drive, even though the browser history had been deleted).

[91] Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary, 110th Cong. 10 (2008) (Statement of Susan K. Gurley, Executive Director of the Association of Corporate Travel Executives).

[92] *Id.* at 11.

[93] *Id.*

[94] *Id.*

[95] *Id.* at 6 (Statement of Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation).

In the absence of an individualized suspicion standard for laptop border searches, there is also the potential for abuse in the form of profiling. This concern was expressed in a recent civil lawsuit filed by the Electronic Frontier Foundation and the Asian Law Caucus.[96] The plaintiff organizations in that lawsuit alleged that the Department of Homeland Security had failed to comply with Freedom of Information Act requests for information on the CBP's border search polices , including any rules that govern the seizure and duplication of the contents of electronic storage devices. This information has since been published, in part, and is available to the public on the CBP's website.[97]

Pretext searches of electronic data pose another concern for international travelers. There have been several cases in which border searches were specifically targeted toward an individual suspected of criminal activity unrelated to national security interests. In *United States v. Pickett*,[98] the defendant, Antonnio Pickett, came to the attention of Immigration and Customs Enforcement agents investigating crimes involving child exploitation and pornography.[99] Picket was *not* an international traveler in the ordinary sense of the term; instead, he was a U.S. citizen employed as a commercial diver with a U.S. contractor performing work in international waters off the coast of Louisiana.[100] Special Agents with ICE believed that evidence of Pickett's involvement in child pornography would be found on his computer, and instead of applying for a warrant, these agents setup a special "secondary customs inspection" at the dock in Louisiana where they knew Pickett's crew boat would return.[101] Relying on the border search exception,

[96] Asian Law Caucus and Electronic Frontier Foundation v. United States Department of Homeland Security, 2008 U.S. Dist. LEXIS 98344 (N.D. Cal. 2008)
[97] U.S. Customs and Border Patrol, Policy Regarding Border Search of Information, http://cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf (July 16, 2008) (last visited April 10, 2010).
[98] 2008 U.S. Dist. LEXIS 69710 (E.D. La. 2008)
[99] *Id.* at 2.
[100] *Id.* at 1.
[101] *Id.* at 2.

special agents searched and viewed the contents of Pickett's thumb drives, portable hard drive, and memory card on one of the laptop computers and discovered child pornography.[102] After his arrest, agents obtained a warrant for another search of the defendant's laptops and computer equipment.[103]

The District Court for the Eastern District of Louisiana held that the search fell within the border search exception and denied Pickett's motion to suppress the evidence.[104] Although Pickett was not an international traveler, the court held that his journey into international waters put him within the authority of customs and made his home dock in Louisiana the "functional equivalent" of the border.[105] Quoting *Arnold*, the court noted that "[r]easonable suspicion is not needed for customs officials to search a laptop or other personal electronic devices at the border."[106] The court also said that it was not necessary to demonstrate that an individual or item actually departed from foreign soil in order to subject it to a customs inspection.[107] In another similar case, the Court of Appeals for the Second Circuit stated that "the validity of a border search does not depend on whether it is prompted by a criminal investigative motive."[108] This court held that pretext should not determine whether a border search is routine or non-routine.[109]

These cases illustrate the potential for misuse of the border search exception to create pretext for a border search where it otherwise would not normally exist. Where law enforcement officers previously had to obtain a warrant to search electronic devices, now they can simply wait for the individual to travel internationally or even to take a deepwater fishing trip in international waters. The thought of returning from a fishing trip to have one's computer,

[102] *Id.* at 2-3.
[103] *Id.* at 3.
[104] *Id.* at 10.
[105] *Id.* at 5.
[106] *Id.* at 8 (quoting *United States v. Arnold*, 523 F.3d 941, 947 (9th Cir. 2008)).
[107] *Id.* at 6
[108] 452 F.3d 110, 123 (2d Cir. 2006).
[109] *Id.*

BlackBerry and USB drives seized with no individualized suspicion would probably prove quite surprising and disturbing to most American citizens and would represent an invasion of traditional notions of privacy.

IV. Constitutionality of the Border Search Exception

The Supreme Court has yet to decide whether suspicionless laptop border searches are permissible under the Fourth Amendment, but prior cases may give us some insight into those factors the Court would likely consider. First in 1977 in *United States v. Ramsey*, and later in 1985, in *United States v. Montoya de Hernandez*, the Court specifically upheld the constitutionality of suspicionless, warrantless border searches of a routine nature.[110] We are therefore left to speculate on whether the Court would consider laptop searches to be routine or non-routine in nature.

In 2006, in *United States v. Flores-Montano*, the Court upheld as routine, a warrantless, suspicionless search of a vehicle that included disassembly and reassembly of a vehicle's gas tank, in part because it considered that search to be noninvasive and because the search did not permanently damage the vehicle.[111] The latitude given to customs officials to perform searches of this nature with no individualized suspicion suggests that the current Supreme Court acknowledges the difficult mission of the Department of Homeland Security and paints the framework of routine border searches quite broadly as a result.

Despite the Court's broad empowerment of U.S. Customs officials, it has also recognized the necessity of limiting some searches that simply go too far.[112] Border searches that are carried out in a particularly offensive manner are considered non-routine.[113] If these searches are not

[110] *Ramsey*, 431 U.S. at 616; *Montoya de Hernandez*, 473 U.S. at 541.
[111] 541 U.S. at 155.
[112] *See Montoya de Hernandez*, 473 U.S. at 540.
[113] *See Flores-Montano*, 541 U.S. at 155, n.2.

supported by reasonable suspicion, the Court's prior decisions suggest that they must be struck down.[114] The Court has not drawn an explicit line between routine and non-routine searches, but it has provided guidance as to specific factors that it may consider in the analysis of laptop border searches.

A. Laptop Border Searches Implicate Dignity and Privacy Interests

In 2004, in *United States v. Flores-Montano*, the Court suggested in dictum, that "the dignity and privacy interests of the person being searched" may "support a requirement of some level of suspicion."[115] Even though a laptop search might not might not seem to intrinsically possess the same level of physical intrusiveness as a body cavity search, most would still consider it a highly personal intrusion.[116] The Supreme Court has held that intrusion is "keyed to embarrassment, indignity, and invasion of privacy" – all factors that are highly relevant in laptop searches.[117] Individuals use laptop computers and other portable electronic storage devices to store massive amounts of data including e-mails correspondence, documents, photographs, videos, passwords, and a variety of personal, professional and financial information.[118] A passenger selected for a random border search of her laptop is likely to feel that her privacy has been invaded. She could also face embarrassment or shame if the highly

---

[114] *Id.*
[115] *Id.* at 152.
[116] *See United States v. Mejia*, 720 F.2d 1378, 1382; *see also United States v. Palmer*, 575 F.2d 721, 723 (9th Cir. 1978) ("Between a search of pockets and a strip search there can be a variety of types of intrusion, which varying degrees of intrusiveness…It is hardly feasible to enunciate a clear and simple standard for each.")
[117] *Id.* (citing *United States v. Sandler*, 644 F.2d 1163, 1167 (5th Cir. 1981)).
[118] *Arnold*, 454 F. Supp. 2d at 1003-04. The trial court listed a number of sensitive types of information commonly stored on laptop computers, stating:

> A laptop and its storage devices have the potential to contain vast amount of information. People keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records. Attorneys' computers may contain confidential client information. Reporters' computers may contain information about confidential sources or story leads. Investors and corporate executives' computers may contain trade secrets.

personal contents of her laptop are viewed by customs officials or even other nearby passengers.[119]

The Ninth Circuit recently recognized that individuals have a legitimate expectation of privacy in their computers. In *United States v. Ziegler*, the court held that individuals have a legitimate expectation of privacy in their workplace computers – affording these computers an expectation of Fourth Amendment protection.[120] This case demonstrates that courts are willing to recognize that "for most people, their computers are their most private spaces," a search of which is a highly invasive personal intrusion.[121]

Another difference that separates laptop searches from less intrusive searches of cargo or luggage is in the reading and collection of information. In an ordinary border search of a traveler's suitcase or vehicle, a customs officer might inspect photographs, documents, identification cards, money, or credit cards – all of which are admittedly personal. "But a laptop search, especially one in which the customs officer opens files, searches through a user's Internet browsing history, and examines his cache or deleted files, is more akin to reading a passenger's diary, [or] reading the contents of international mail…"[122] A document composed on, or scanned into a computer is no less deserving of protection than a document printed on paper.[123]

Adding to the invasiveness of the search of these personal documents is the customs officer's ready ability to copy and store all of that information for later examination, as well as the ability to access documents and files which have been deleted by the traveler. Thus although

---

[119] *Id.*; *see also United States v. Braks*, 842 F.2d 509, 511-12 (1st Cir. 1988)
[120] 474 F.3d 1184 (9th Cir. 2007)
[121] *Id.* at 1189 (quoting *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006).
[122] Coletta, Chrstine A., 48 B.C.L. Rev. 971, 1000 (2007).
[123] In a dissenting opinion, Chief Judge Kozinski of the Ninth Circuit argued that the Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, *papers*, and effects…" *United States v. Seljan*, 547 F.3d 993, 1014 (9th Cir. 2008) (emphasis supplied). By affirming the defendant's conviction based on a warrantless and suspicionless customs search of outgoing packages at a FedEx sorting facility, Judge Koziniski argued that the majority was ignoring this clause of the Fourth Amendment and disregarding "the Founders' deep concern with safeguarding the privacy of thoughts and ideas…from invasion by the government." *Id.*

a traveler can take steps to remove data or mitigate access to his information, in many cases these safeguards can be circumscribed by customs inspectors using readily available forensic tools. Accessing deleted data which normally exists only as inaccessible digital bits on a hard drive is akin to accessing the thoughts and memories of an individual which exist only as unconsciously encoded neural connections within the brain.[124] The only way a traveler can truly protect their data is to leave it at home – a solution which is impractical at best for most travelers. Thus the unique nature of digital data adds to privacy concerns.

In light of these intrusive invasions of privacy, laptop border searches should be characterized as non-routine. The nature and volume of information contained on even the smallest of electronic storage devices dwarfs that which could be readily inspected, read and analyzed during a routine border search of a person or their luggage, and can reveal much more personal and private information about the individual.[125] This information implicates the dignity and privacy rights of U.S. citizens and non-citizens alike. Although proponents of the border search exception have noted its success in apprehending child pornography and its importance in securing the nation's borders, the issue must be considered in light of its impact on the general public.

B. The Scope of Routine Border Searches Should be Consistent with Their Justification

Even if the Court refuses to categorize laptop searches as non-routine, prior case law suggests that the scope of the search should be consistent with the justifications supporting the Fourth Amendment exception in the first place. Each time the Court has established a new exception to the warrant or probable cause requirements of the Fourth Amendment, it has

[124] See Robert J. Sternberg, Cognitive Psychology, 196 (4th ed. 2006).
[125] *See Arnold*, 454 F. Supp 2d at 1000 ("[e]lectronic 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").

delineated its reasons for doing so. Often, warrantless searches are based on a finding of exigent circumstances. Other times, the Court does away with the warrant requirement entirely because the policies behind that requirement are not implicated in a particular type of search.[126] Border searches, on the other hand, have been explained as the result of the unique power of the federal government, as sovereign, to control who and what crosses its borders.[127] The Court has stated that Congress has given "the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."[128]

In *Terry v. Ohio*, the Court upheld the constitutionality of the warrantless "stop" and "frisk" procedure based on a justification of officer and public safety.[129] In an opinion written by Chief Justice Warren, the court warned that the scope of the search must be consistent with the justification for the Fourth Amendment exception: "The sole justification of the search…is the protection of the police officer and others nearby, and it must therefore be confined in scope to an intrusion reasonably designed to discover guns, knives, clubs, or other hidden instruments for the assault of the police officer."[130]

Like the common stop and frisk search in *Terry*, border searches must also remain consistent with their historical justification of preventing the entry of illegal aliens and contraband.[131] Furthermore, these searches must be reasonably designed and narrowly tailored to fit that mission. In the CBP's "Policy Regarding Border Search of Information," published in

---

[126] *Colorado v. Bertine*, 479 U.S. 367, 371 (1987) (upholding the constitutionality of warrantless inventory searches because "[t]he policies behind the warrant requirement are not implicated in an inventory search, nor is the related concept of probable cause…")
[127] *Ramsey*, 431 U.S. at 620 (1977)
[128] *Montoya de Hernandez*, 473 U.S. at 537.
[129] *Terry v. Ohio*, 392 U.S. 1, 29 (1968)
[130] *Id.* ("[E]vidence may not be introduced if it was discovered by means of a seizure and search which were not reasonably related in scope to the justification for their initiation." (citing *Warden v. Hayden*, 387 U.S. 294, 310 (1967))).
[131] Alzahabi, Rasha, 41 Ind. L. Rev. 161, 176 (2008).

2008, the agency states that its examination of "documents, books, pamphlets, and other printed material, as well as computers, disks, hard drives, and other electronic or digital storage devices" is part of "CBP's long-standing practice and [is] essential to uncovering vital law enforcement information."[132] However, this document misstates the traditional rationale behind the border search exception and demonstrates the unreasonable, loosely tailored rationale that has developed to justify a new breed of border searches . "[U]ncovering vital law enforcement information" is a gross exaggeration of the historical justification for the border search exception – to collect duties and to prevent the introduction of contraband into the country.[133]

Of course, the government does have a strong interest in finding and investigating electronic information relating to terrorism and other national security concerns, but this should not be enough to erode the basic constitutional protections of the Fourth Amendment. Its digital nature means that the information contained within a laptop computer or other electronic storage device can be transported across our borders and across the world, regardless of whether an individual ever enters or leaves the country. For example, in *Romm*, the photos found on the defendant's computer had been downloaded from a child pornography website.[134] These same photos could have been accessed with the click of the mouse by Romm or anybody else, from anywhere in the world. Remote access solutions designed by businesses to protect their employees from suspicionless laptop border searches prove that information does not have to cross the border to enter the country.[135] Just as business travelers can take advantage of the internet's versatility and worldwide accessibility, so too can terrorists and others who pose a

[132] U.S. Customs and Border Patrol, Policy Regarding Border Search of Information, http://cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf (July 16, 2008) (last visited April 10, 2010).
[133] *Montoya de Hernandez*, 473 U.S. at 537.
[134] *Romm*, 455 F.3d at 994.
[135] Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary, 110th Cong. 11 (2008) (Statement of Susan K. Gurley, Executive Director of the Association of Corporate Travel Executives).

threat to our national security. The free flow of information over the Internet calls into question the efficacy of border laptop searches as a defense in the war on terror, as well as it's justifications in other regards.

A compromise between privacy interests and the government's interest as sovereign can be met by requiring a relatively low degree of individualized suspicion for in depth border searches of electronic data. The rest of the world looks to the United States as an example of democracy and freedom. Since customs agents are some of the first faces to greet new arrivals to America, it is important that we maintain this reputation – especially in the face of terrorists who seek so badly to harm it.

V. New Technology Requires New Protections

Computers may be a relatively recent technology in the eyes of the law, but the Supreme Court is no stranger to interpreting the Constitution in light of advances in technology. The first notable case in which the Court examined the legal implications of a new technology was *Katz v. United States.*[136] In *Katz*, the Court held that warrantless audio surveillance on a public telephone booth violated the defendant's Fourth Amendment rights.[137] "One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouth piece will not be broadcast to the world."[138] The Court further explained that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[139]

[136] 389 U.S. 347 (1967).
[137] *Id.* at 359.
[138] *Id.* at 352.
[139] *Id.*

Public telephones have largely fallen out of use – they no longer play such a vital role in private communication.[140] But in their place, cellular telephones, iPhones, BlackBerry messaging devices and laptop computers have risen to fill this role. To ignore the expectation of privacy that an individual has in these devices, would be to ignore the vital role that new technology plays in private communication.

The Court affirmed its concern that new technologies can lead to diminished privacy in *Kyllo v. United States*.[141] The issue in *Kyllo* was whether "a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment."[142] The Court held that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."

As is *Katz*, the Court in *Kyllo* recognized the important impact technology has on every citizen's right to privacy. The types and amount of information contained within a laptop computer are akin to the information that could be found by a search of an individual's home. Although technology has made it possible to gain access to this information without physical intrusion of the type that typically requires a warrant, courts must protect rights of privacy and dignity and require at least some degree of individualized suspicion in order to search laptop computers and other electronic devices.

VI. Conclusion

[140] AT&T, AT&T Announces Intention to Withdraw from Pay Phone Business by End of 2008. (December 3, 2007) http://www.att.com/gen/pressroom?pid=4800&cdvn=news&newsarticleid=24840 (last visited May 10, 2010)
[141] 533 U.S. 27 (2001).
[142] *Id.* at 29.

The government's power to regulate the flow of people and goods across the borders is more important today than ever before. It's also more challenging. Customs and Border Patrol welcomes over 1.1 million travelers into the United States *each day*.[143] These travelers come by air, land and sea. The Supreme Court, as well as lower federal courts, has acknowledged the difficult job facing customs agents and the importance of their mission. In response, the courts have granted customs officials broad authority to conduct routine searches without any individualized suspicion at the borders. Those same courts have also placed certain reasonable limits upon these searches, holding that when a border search is non-routine, because it is overly invasive, intrusive or implicates privacy and dignity concerns, reasonable suspicion is required before a search can take place.

Laptop computers and other electronic devices are fundamentally different from those items typically considered eligible for routine searches at the border. They contain a great deal of highly personal information which implicates dignity and privacy interests. For this reason, the search of laptops and other electronic devices should be considered non-routine, and should require customs officials to demonstrate some level of reasonable suspicion prior to performing a search.

This relatively easy to prove standard of reasonable suspicion is the ideal compromise between the government's interest in national security and the individual privacy interests of persons crossing the border. In fact, in the majority of the case law on this topic, the court never had to reach a determination of routine or non-routine because the searches were found to have been based on reasonable suspicion.[144]

---

[143] Customs and Border Patrol, CBP Travel Spotlight, http://www.cbp.gov/xp/cgov/travel (last visited April 12, 2010)

[144] See United States v. Irving, 452 F.3d 110 (2006); United States v. Furukawa, 2006 U.S. Dist. LEXIS 83767 (Minn. Dist. 2006); United States v. Bunty, 617 F. Supp. 2d 359 (E.D.P.A. 2008).

Although one can only speculate on how this issue would be decided by the Supreme Court, there is no doubt that future courts will have to take into account the ever expanding importance of technology in regards to the privacy interests of individuals.