Brooklyn Law Review

Volume 72 | Issue 2 Article 9

2007

Preserving the Border Search Doctrine in a Digital World: Reproducing Electronic Evidence at the Border

Kelly A. Gilmore

Preserving the Border Search Doctrine in a Digital World

REPRODUCING ELECTRONIC EVIDENCE AT THE BORDER

I. INTRODUCTION

On September 23, 1997, a man arrived with his family at John F. Kennedy International Airport in New York ("JFK") en route to his suburban home in Arlington, Texas.[1] The traveler, Wadih El-Hage, was detained by U.S. Customs officials[2] who proceeded to search his luggage and photocopy materials found therein before returning his belongings and

---

[1] United States v. Bin Laden, No. S(7) 98 CR. 1023, 2001 WL 30061, at *2 (S.D.N.Y. Jan. 2, 2001); Oriana Zill, *A Portrait of Wadih El Hage, Accused Terrorist*, PBS Frontline, http://www.pbs.org/wgbh/pages/frontline/shows/binladen/upclose/elhage.html (last visited Aug. 30, 2006).

[2] In March 2003, the United States Customs Service was transferred from Treasury Department control to the newly created Department of Homeland Security ("DHS"). *The Future is Now*, U.S. CUSTOMS TODAY (U.S. Customs Serv., Washington, D.C.), Feb. 2003, *available at* http://www.cbp.gov/xp/CustomsToday/2003/February/future.xml. The Service, renamed the Bureau of Customs and Border Protection ("CBP"), joined twenty-two federal agencies under the new department including the Federal Emergency Management Agency, the Transportation Security Administration, the U.S. Coast Guard, and the U.S. Secret Service. CBP is a consolidation of the former U.S. Customs Service, the U.S. Border Patrol, the Immigration and Naturalization Service, and the Animal and Plant Health Inspection Service. The agency currently functions under the Border and Transportation Security directorate within Homeland Security and shares responsibilities with two sister agencies: Immigration and Customs Enforcement ("ICE") and U.S. Citizenship and Immigration Services ("USCIS"). CBP is largely responsible for preventing the import and export of contraband while facilitating the flow of legitimate trade and travel; ICE operates as the largest investigative arm of Homeland Security; and USCIS is responsible for the administration of immigration and naturalization adjudication functions. DHS, Department Subcomponents and Agencies, http://www.dhs.gov/dhspublic/display?theme=9 (last visited Aug. 30, 2006).

Homeland Security governs over 170,000 workers and is the third largest employer in the executive branch following the Defense Department and the Department of Veterans Affairs. Philip Shenon, *Threats and Responses: The Reorganization Plan; Establishing New Agency is Expected to Take Years and Could Divert It from Mission*, N.Y. TIMES, Nov. 20, 2002, at A14.

Throughout this note, Customs and Border Protection officers will be referred to as both "Customs officials" and "CBP officials" since earlier case law retains the former terminology.

allowing him to continue his journey.[3] El-Hage was later named one of fifteen defendants charged with 267 discrete criminal offenses in connection with the 1998 bombings of the United States Embassies in Nairobi, Kenya and Dar es Salaam, Tanzania.[4] El-Hage's effort in a later criminal proceeding to suppress the photocopied evidence as "fruit of the poisonous tree"[5] was denied by the Southern District Court of New York.[6] The Court rejected his claim that the JFK search was a violation of the Fourth Amendment, thus tainting the evidence obtained.[7] The Court concluded that not only was the initial search valid, but the mass reproduction of his documents was constitutionally permissible.[8]

For illustrative purposes, imagine the individual searched is not an alleged member of an international terrorist network, but simply the occasional traveler returning home from a popular vacation spot such as Mexico or Jamaica.[9] Customs and Border Protection (CBP) officers do not search the papers he or she may be carrying in his or her briefcase or pocketbook. Instead, they search a BlackBerry[10] containing

---

[3] *Bin Laden*, 2001 WL 30061, at *2.

[4] United States v. Bin Laden, 92 F. Supp. 2d 225, 227 (S.D.N.Y. 2000). On August 7, 1998, simultaneous bombs at the two embassies killed 224 people (including twelve Americans) and injured thousands. David Johnston & Andrew C. Revkin, *Threats & Responses: The Methods; Officials Say Their Focus is on Car and Truck Bombs*, N.Y. TIMES, Aug. 2, 2004, at A13.

El Hage was convicted in May 2001 of conspiracy to kill United States nationals and perjury for statements made during a grand jury proceeding. Zill, *supra* note 1. El Hage and three co-conspirators, Mohamed Rashed Daoud al-'Owahli, Khalfan Khamis Mohamed, and Mohammed Saddiq Odeh, were sentenced to life in prison without the possibility of release. Benjamin Weiser, *A Nation Challenged: The Courts; 4 Are Sentenced to Life in Prison in 1998 U.S. Embassy Bombings*, N.Y. TIMES, Oct. 19, 2001, at A1.

El Hage, a naturalized U.S. citizen, is believed to have been one of Osama bin Laden's top aides. *See* Zill, *supra* note 1. Allegedly bin Laden's personal secretary, El Hage maintains that he only assisted the al Qaeda leader in his legitimate business affairs which included a tannery, farms, a construction firm, a transport business, and two investment companies. *Id.*

[5] *See generally* Wong Sun v. United States, 371 U.S. 471 (1963) (establishing the "fruit of the poisonous tree" doctrine, which states that underlying police misconduct that violates the Fourth Amendment may taint evidence obtained by law enforcement, thus making it inadmissible).

[6] *Bin Laden*, 2001 WL 30061, at *3-4.

[7] *Id.* at *4.

[8] *Id.* at *4 n.7.

[9] *See infra* note 240 and accompanying text.

[10] A BlackBerry is a hand-held, wireless internet device manufactured by the Canadian company Research in Motion. *See* BlackBerry, http://www.blackberry.com (last visited Oct. 20, 2006). With an estimated 200 million users in the United States, the BlackBerry plays a critical role in the operation of the nation's leading industries

months worth of personal communications and business related emails, or an iPod with over 20,000 personal photographs as well as an organizer and address book.[11] The officers then proceed to download and copy the electronically stored information before returning the device and allowing the passenger to continue his or her trip home. This scenario gives rise to privacy concerns not likely to be encountered during a traditional inspection of paper documents. The quantity and quality of personal materials that can be stored in a personal digital assistant (PDA) or laptop computer appears to make the search and duplication of digital information substantially more invasive.[12] The hypothetical inspection described above seems excessive and unjustified, however, this note will demonstrate that it is not. CBP's authority to inspect laptop computers or electronic hand-held devices and to subsequently reproduce files contained therein is not only constitutionally permissible but essential for the effective policing of our international border. In the digital era, the advent of the mobile electronics market has given individuals the ability to conceal incriminating evidence effortlessly—information that may be needed for the successful prosecution of hundreds of different federal criminal offenses.[13] CBP must be able to respond to this threat.

The Supreme Court has recently indicated that objects such as vehicles may be searched at the border without reasonable suspicion.[14] A similar approach has been used to validate the suspicionless border search of computers and computer disks, holding that the inspection of these devices may be equated with the examination of traditional carry-on items.[15] Additionally, CBP has the authority to photocopy paper documents such as letters, address and date books, and

---

and professions, including Wall Street. Paul Taylor, *RIM Pleads for BlackBerry in Patent Case*, FIN. TIMES (U.S.A.), Jan. 19, 2006, at 23.

[11] *See infra* Part V.A.

[12] *Id.*

[13] In addition to its own regulations, CBP is responsible for enforcing over 400 laws on behalf of over forty federal agencies. CBP, CBP Cargo Examinations, http://cbp.gov/xp/cgov/border_security/port_activities/cargo_examinations.xml (last visited July 31, 2006).

[14] United States v. Flores-Montano, 541 U.S. 149, 152-55 (2004).

[15] *See, e.g.*, United States v. Ickes, 393 F.3d 501, 504 (4th Cir. 2005) (upholding the border search of laptop computers as reasonable inspection of cargo).

receipts examined during routine searches.[16] Only the *reproduction* of those materials is subject to a standard of reasonable suspicion; the initial inspection is not.[17] This note will argue that the authority to reproduce paper material, when read in light of recent decisions concerning inanimate objects and electronic equipment, must be extended to allow for the reproduction of digital information stored in laptops, flash drives, memory sticks, and PDAs during a border search. Despite heightened privacy concerns regarding the volume of personal communications that may be stored within computers and hand-held devices, this note will demonstrate that the extension of this authority is critical to the maintenance of border integrity and the security of our nation in an increasingly digitalized world.[18] The appropriate solution to address these privacy concerns is not to restrict CBP border search authority or the ability to reproduce evidence found during an inspection. Instead, the Agency must adopt a policy of non-retention and non-dissemination when the replicated evidence is deemed no longer to have evidentiary, prosecutorial, or investigative value.[19] This proposal, coupled with the inherent limits of CBP enforcement powers, will be more than sufficient to ensure that border inspection authority is not eroded while simultaneously protecting the privacy interests of those international travelers who have not violated federal law.[20]

Part II of this note will provide an overview of the Fourth Amendment's prohibition of unreasonable searches and seizures[21] and explain how this constitutional protection is

---

[16] *See, e.g.*, United States v. Fortna, 796 F.2d 724, 738-39 (5th Cir. 1986); United States v. Soto-Teran, 44 F. Supp. 2d 185, 191 (E.D.N.Y 1996), *aff'd*, 159 F.3d 1349 (2d Cir. 1998); State v. Codner, 696 So. 2d 806, 810-11 (Fla. Dist. Ct. App. 1997).

[17] United States v. Bin Laden, No. S(7) 98 CR. 1023, 2001 WL 30061, at *4 n.7 (S.D.N.Y. Jan. 2, 2001) (citing *Soto-Teran*, 44 F. Supp. 2d at 185, 191). Reasonable suspicion is defined as "'a particularized and objective basis for suspecting the [specific individual]' of . . . smuggling." United States v. Montoya de Hernandez, 473 U.S. 531, 541-42 (1985) (quoting United States v. Cortez, 449 U.S. 411, 417 (1981)).

[18] Customs officers are in a unique law enforcement position. While they do not have general police powers, officers do have the opportunity "to look for evidence of . . . wrongdoing [and to present such evidence] obtained during a valid border search to criminal prosecutors." Jon Adams, *Rights at United States Borders*, 19 BYU J. PUB. L. 353, 366-67 (2005). However, the evidence is still subject to exclusionary rules if it was obtained through CBP misconduct. *Id.* at 367. See *infra* Part IV.B for further discussion of the limits on CBP officers' powers.

[19] *See* Heidy v. U.S. Customs Serv., 681 F. Supp. 1445, 1453 (C.D. Cal. 1988).

[20] *See infra* Part V.D.

[21] U.S. CONST. amend. IV.

inapplicable at the United States international border or its functional equivalent.[22] This section will explain the traditional distinctions between various types of border searches and the suspicion-less standard adopted by the Supreme Court regarding the search of personal property.[23] Part III will examine the ability of CBP officials to search laptop computers and diskettes under this framework.[24] Part IV will examine the government's authority established by *United States v. Fortna*[25] not only to search personal property but to photocopy paper material as well.[26] This section will explore the scope of the *Fortna* decision as well as the limits placed on the government's ability to copy,[27] retain, and disseminate such material.[28] Part IV will conclude by applying the *Fortna* holding to electronically stored information. This section will explain that current case law regarding photocopying, when correctly read together with the recent decisions concerning laptop searches, creates the ability to reproduce electronic files under a standard of reasonable suspicion. Part V will demonstrate the critical need for this enhanced authority and refute several arguments to the contrary. Section A will address the unique nature of electronic devices, namely the storage capacity that raises privacy concerns for travelers and presents a unique law enforcement challenge to Customs. Section B will address the

---

[22] An example of what is deemed the functional equivalent of the international border would be an airport serving as the final destination for a nonstop international flight. United States v. Gaviria, 805 F.2d 1108, 1111 (2d Cir. 1986). A functional equivalent may also be at a point marking the confluence of two or more roads extending from the actual border. Almeida-Sanchez v. United States, 413 U.S. 266, 272-75 (1973) (holding a search conducted twenty-five miles from the United States border did not occur at the functional equivalent despite the fact that it was a highway route commonly used by undocumented noncitizens).

[23] United States v. Flores-Montano, 541 U.S. 149, 155 (2004).

[24] *See, e.g.*, United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) (holding that laptop computers are "cargo" within the meaning of searchable items under 19 U.S.C. § 1581(a) (2000)).

[25] 796 F.2d 724 (5th Cir. 1986).

[26] This authority includes the inspection and reproduction of both outbound and inbound materials sent through shipping services not accompanying a passenger traveling internationally. *See* United States v. Seljan, 328 F. Supp. 2d 1077, 1082 (C.D. Cal. 2004).

[27] *See* People v. LePera, 611 N.Y.S.2d 394, 395-96 (App. Div. 1994) (holding that the copying of materials during a border search is limited to the laws customs officials may enforce).

[28] *See, e.g.*, Heidy v. U.S. Customs Serv., 681 F. Supp. 1445, 1449-50 (C.D. Cal. 1988) (holding that photocopies of non-seditious material obtained during a valid border search were not to be retained by law enforcement agencies); *see also infra* Part V.D.

fact that despite concerns regarding the disclosure of personal information, there is no reasonable expectation of privacy in the border context. Section C will examine the devastating consequences of the failure to apply the *Fortna* holding to digital information. Finally, Section D will conclude by emphasizing that existing protections and the implementation of a non-retention policy adequately serve the interests of both CBP and international travelers.

II. THE BORDER SEARCH DOCTRINE

A. An Exception to the Fourth Amendment

The Fourth Amendment guarantees that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[29]

This protection was created largely as a response to the English and colonial era law enforcement practice of entering private homes and conducting invasive searches for criminal evidence without probable cause.[30] By including this safeguard in the Bill of Rights, the drafters wished to ensure that such intrusive, unreasonable violations of legitimate privacy expectations[31] did not occur in the United States unless certain preliminary requirements were met.[32] The Fourth Amendment mandates that a warrant be issued based on probable cause

---

[29] U.S. CONST. amend. IV.

[30] *See* Payton v. New York, 445 U.S. 573, 583 (1980) ("It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." (citing Boyd v. United States, 116 U.S. 616, 625 (1886)); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 536 (2005).

Probable cause is established when the magistrate issuing the warrant determines that "there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 214 (1983).

[31] A search occurs when an expectation of privacy that society considers reasonable is infringed. Laura Hill, Note, *To Squeeze or Not to Squeeze?: A Different Perspective*, 37 TULSA L. REV. 425, 426 (2001) (discussing the Supreme Court's "no squeeze" rule as applied to law enforcement officers' ability to search luggage on buses).

[32] *See* Kerr, *supra* note 30, at 536.

prior to commencing the search.[33] The warrant must not only describe the place to be searched but also the person or things to be seized.[34] The unreasonable search of a person's home remains the principal evil against which the Fourth Amendment is directed.[35] The government may enter one's personal abode to search and seize possessions only if it has obtained a warrant or an exception applies to the particular situation.[36] However, this protection is not an absolute constitutional right.[37] Its application necessarily hinges on the reasonableness of an individual's expectation of privacy in a given situation.[38]

At the United States border or its functional equivalent, there is no reasonable expectation of privacy; an exception to the Fourth Amendment applies.[39] Historically, the Executive branch and specifically the U.S. Customs Service have enjoyed plenary power at the border.[40] There exists a "longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' [and have] a history as old as the Fourth Amendment itself."[41] In

---

[33] *See Payton*, 445 U.S. at 584 ("As it was ultimately adopted . . . the [Fourth] Amendment . . . require[s] that warrants be particular and supported by probable cause."); Ybarra v. Illinois, 444 U.S. 85, 92 (1979) ("The Fourth amendment directs that 'no Warrants shall issue but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized.'" (quoting U.S. CONST. amend IV)); *see also* Kerr, *supra* note 30, at 536.

[34] *Ybarra*, 444 U.S. at 92 (citing U.S. CONST. amend. IV).

[35] United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972) (holding unlawful the electronic surveillance of defendant's conversations without prior judicial approval).

[36] *See* Kerr, *supra* note 30, at 536.

[37] "[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." Katz v. United States, 389 U.S. 347, 357 (1967) (footnote omitted) (holding that a person may reasonably rely on the protections of the Fourth Amendment when he or she enters a public telephone booth to have a private conversation).

[38] *Id.* at 361 (Harlan, J., concurring).

[39] United States v. Flores-Montano, 541 U.S. 149, 154 (2004) (citing United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985)).

[40] Customs officials may board vessels and search any "vehicle, beast, or person" suspected of illegally bringing goods into the United States, 19 U.S.C. § 482 (2000), and further, CBP officers may inspect the baggage of all persons arriving in the United States, 19 U.S.C. § 1496 (2000). Other federal officials may be authorized to conduct border searches as well. *See, e.g.*, 14 U.S.C. § 89(a) (2000) (permitting Coast Guard officials to make inspections, searches, and seizures on the high seas and all other waters within U.S. jurisdiction); United States v. Victoria-Peguero, 920 F.2d 77 (1st Cir. 1990) (holding that a Puerto Rican drug unit was authorized under 19 U.S.C. § 1401(i) (2000) to make customs seizures).

[41] United States v. Ramsey, 431 U.S. 606, 619 (1977). The first customs statute, Act of July 31, 1789, c. 5, 1 Stat. 29, was passed by the same Congress that

United States v. Montoya de Hernandez, the Supreme Court explained the justification for this broad authority, citing the inherent right of an independent, sovereign nation to protect itself by examining the people and articles moving in or out of the country.[42] The Court upheld the authority of Customs to detain a suspected cocaine smuggler and emphasized that searching people and their affects is critical national security.[43] At the international border, the federal government's obligations to collect duties and its protectionist interest in preventing the entry of stolen goods[44] and controlled substances[45] is at its "zenith."[46] The sovereign's compelling security interests must be balanced against the Fourth Amendment's protections and the privacy rights of arriving or departing individuals and their personal property.[47] At the border, the scales clearly tip in the government's favor.[48]

B. The Distinction between Routine and Non-Routine Border Searches

Within the border search context, inspections have typically been characterized as either suspicion-less and routine, or physically invasive and non-routine.[49] In order to conduct routine border searches, Customs inspectors do not

---

would present a proposal for the Fourth Amendment to state legislatures less than two months later. *Id.* at 616. This statute distinguished those searches which take place in the interior and require a warrant upon probable cause from those which are required at the border to enforce customs laws and duties, giving Customs nearly plenary power at the border. *Id.* at 616-17.

> As this Act was passed by the same Congress which proposed for adoption the original amendments to the Constitution, it is clear that the members of that body did not regard searches and seizures of this kind as 'unreasonable,' and they are not embraced within the prohibition of the amendment.

Id. at 617 (quoting Boyd v. United States, 116 U.S. 616, 623 (1886)). Thus, the notion that border searches are exempt from Fourth Amendment requirements is well established and has long been embraced by the Supreme Court. *Id.*

[42] *Montoya de Hernandez*, 473 U.S. at 538.

[43] *Id.*

[44] *Ramsey*, 431 U.S. at 618 (quoting Carroll v. United States, 267 U.S. 132, 153-54 (1925)).

[45] *Montoya de Hernandez*, 473 U.S. at 538 (citing United States v. Mendenhall, 446 U.S. 544 (1980) (Powell, J., concurring)).

[46] United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

[47] *See* United States v. Berisha, 925 F.2d 791, 794-95 (5th Cir. 1991) (holding that the border search exception to the Fourth Amendment applies equally to persons departing from the United States).

[48] *Montoya de Hernandez*, 473 U.S. at 539-40.

[49] *See id.* at 538-41.

need to produce a warrant, show probable cause, or even possess reasonable suspicion.[50] Accordingly, CBP officers may search carry-on bags and checked luggage, conduct canine sniffs or pat-downs,[51] photograph and fingerprint travelers,[52] and even disassemble the gas tank on a vehicle without an independent trigger[53] for the search.[54] Non-routine searches on the other hand, are characterized by a more physically intrusive nature and typically involve procedures such as strip searches, body cavity searches, involuntary x-rays, and physical detention.[55] These inspections implicate the Fourth

---

[50] *Id.* at 538. *See also* United States v. Singh, 415 F.3d 288, 293 (2d Cir. 2005) (explaining that routine searches at the border are viewed as reasonable *per se* requiring neither a warrant nor probable cause).

Traditionally, the classification of a border search depended on the degree of invasion. In the context of property searches, courts are generally unwilling to find a sufficient degree of intrusiveness to raise a search to the level of non-routine, thus requiring reasonable suspicion. *See, e.g.*, United States v. Villamonte-Marquez, 462 U.S. 579, 592-93 (1983) (holding that boats in inland waters with access to the sea may be stopped and boarded without suspicion); United States v. Martinez-Fuerte, 428 U.S. 543, 562 (1976) (holding that vehicles may be stopped at check points near the border without any standard of suspicion and such an inspection may be categorized as routine); United States v. Cortez-Rocha, 394 F.3d 1115 (9th Cir.) (affirming the validity of a border search that required the cutting open of vehicle's tire), *cert. denied*, 126 S. Ct. 105 (2005); United States v. Myers, 127 F. App'x 251, 252-53 (9th Cir. 2005) (holding that the drilling of a small hole into a the bed of a truck was not destructive and not did it affect the vehicle's operation; reasonable suspicion was not required).

[51] A number of circuit courts have held pat-downs to be part of a routine, suspicionless border search. *See e.g.*, Bradley v. United States, 299 F.3d 197, 203 (3d Cir. 2002); United States v. Beras, 183 F.3d 22, 26 (1st Cir. 1999); United States v. Gonzalez-Rincon, 36 F.3d 859, 864 (9th Cir. 1994); United States v. Carreon, 872 F.2d 1436, 1442 (10th Cir. 1989); United States v. Oyekan, 786 F.2d 832, 835 (8th Cir. 1986). Canine sniffs are also considered routine. *See* United States v. Cedano-Arellano, 332 F.3d 568 (9th Cir. 2003).

[52] Tabbaa v. Chertoff, No. 05-CV-582S, 2005 WL 3531828, at *11 (W.D.N.Y. Dec. 22, 2005) (stating that fingerprinting and photographing may be part of "a minimally invasive routine search" and that "fingerprinting is a tool used by the government to discharge its duty of verifying the identity and admissibility of those who present themselves for admission to the United States").

[53] Independent circumstances which may arouse an agent's suspicions include: excessive nervousness, unusual conduct, traveling to or from a narcotics source country, tips from informants, inadequate luggage, loose-fitting clothing, contradictory answers, lack of employment, claim of self employment, or airline tickets paid for in cash. *See* Adams, *supra* note 18, at 364-65 (exploring the scope of the border search doctrine and its value).

[54] *See* United States v. Flores-Montano, 541 U.S. 149, 155 (2004) (holding that the disassembly and reassembly of a vehicle's fuel tank was routine); United States v. Chaudhry, 424 F.3d 1051, 1051 (9th Cir. 2005) (affirming that the drilling of a small hole in the bed of a pick up truck to search for contraband did not require reasonable suspicion), *cert. denied*, 126 S. Ct. 1803 (2006); United States v. Hernandez**,** 424 F.3d 1056, 1057 (9th Cir. 2005) (affirming that removal of vehicle door panels with screw driver was routine search, reasonable suspicion not required).

[55] *See Montoya de Hernandez*, 473 U.S. at 541 & n.4 (holding that the twenty-seven hour detention of a Colombian national suspected of alimentary canal smuggling

Amendment and may be subject to a reasonable suspicion standard.[56] In *Montoya de Hernandez*, the Supreme Court clarified the distinction between the two types of searches and determined that the monitored detention of a Colombian national suspected of alimentary canal smuggling required only the reasonable suspicion of Customs inspectors.[57]

The Court explained that CBP officers must be held to a higher standard of suspicion for physically invasive searches and those resulting in detention.[58] However, the Court also emphasized that demanding anything more than reasonable suspicion is impracticable.[59] Illegal behavior at the border, such as internal narcotics smuggling, will rarely produce external symptoms.[60] Federal violations undetectable by outward, physical signs may range from the possession and transportation of child pornography[61] to evidence of participation in a drug trafficking conspiracy.[62] Direct evidence of such violations may also be concealed in laptop computers or

---

was appropriate based on the reasonable suspicion of Customs officers). The Court in *Montoya de Hernandez* provided several examples of searches intrusive enough to be characterized as non-routine. *Cf.* United States v. Okafor, 285 F.3d 842, 845-46 (9th Cir. 2002) (explaining that the x-ray examination of luggage and other containers at the border is routine and does not require individualized suspicion); United States v. Lawson, 374 F. Supp. 2d 513 (E.D. Ky. 2005) (same), *aff'd*, 461 F.3d 697 (6th Cir. 2006).

[56] *Montoya de Hernandez*, 473 U.S. at 541.

[57] *Id.* The Court explained that to hold CBP officials to a higher standard of suspicion would be unreasonable. *Id.* The government's interest in preventing illegal narcotics from entering the country is high and such techniques as alimentary canal smuggling present no external signs that will enable officials to act on anything more than an objective, reasonable suspicion, which is often based on years of experience. *Id.* at 541-42.

[58] *Id.*

[59] *Id.* at 541. Frisks or strip searches will not uncover alimentary canal smuggling and detention to confirm suspicions or dispel them is an option preferable to releasing the suspect into the interior with contraband. *Id.* at 543-44.

[60] *See, e.g.*, Blackwood v. State, 581 S.E.2d 724, 725 (Ga. Ct. App. 2003) (noting that defendant who had ingested more than one pound of cocaine displayed no outward signs of smuggling).

[61] 18 U.S.C. § 2252A(a)(5)(B) (2000) makes it unlawful for anyone to "knowingly possess[] any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer." Such offense is punishable by fine, and an offender may be imprisoned for a maximum term of twenty years. *See* 18 U.S.C. § 2252A(b).

[62] 21 U.S.C. § 841(a) (2000) makes it unlawful for any person knowingly or intentionally "(1) to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance; or (2) to create, distribute, or dispense, or possess with intent to distribute or dispense, a counterfeit substance." Persons convicted of conspiracy or attempt of section 841 are "subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy." 21 U.S.C. § 846 (2000).

PDAs. Thus, reasonable suspicion is often the most officers will be able to demonstrate; anything else is simply unworkable in practice. Demanding compliance with a higher standard of suspicion would allow for widespread evasion of federal law.[63] In light of the compelling government interests in protecting its territorial borders and the inability of Customs officials to show probable cause, imposing a higher burden on CBP would vitiate the purpose of the border search doctrine.[64]

C. The Flores-Montano *Approach*

While the routine/non-routine distinction may remain important to the validity of physically invasive border searches, the Supreme Court has recently rejected the notion that "complex balancing tests" be used to characterize Customs inspections, at least in the context of vehicles.[65] In *United States v. Flores-Montano*, the Court held that the disassembly of a vehicle's gas tank was a routine border search and individualized suspicion was not required.[66] The decision overruled nearly thirty years of case law imposing a reasonable suspicion standard on such actions.[67] Customs officers had stopped a station wagon attempting to enter the United States at the Otay Mesa Port of Entry in southern California.[68] As

---

[63] *See Montoya de Hernandez*, 473 U.S. at 543.

[64] The reasonable suspicion standard fits well within this border search context, effectively balancing private interests against the compelling governmental interest in stopping smuggling at the border. *Id.* at 541-42.

Related to non-routine border inspections at the international border or its functional equivalent is the extended border search which occurs *near* the border and is constitutionally permissible if the following three-prong test is met: (1) there is a reasonable certainty that a border crossing has occurred; (2) there is a reasonable certainty that no change in condition of the luggage has occurred since the crossing; and (3) there is a reasonable suspicion that criminal activity has occurred. *See* United States v. Caminos, 770 F.2d 361, 364 (3d Cir. 1985). In *United States v. Yang*, the court held that the search of a defendant at another airport terminal after the individual had passed through Customs was lawful under the extended border search doctrine, since the three requirements explained above had been met, and officers had already discovered a significant amount of drugs on his traveling companion. 286 F.3d 940, 943, 945, 949 (7th Cir. 2002). *See also* United States v. Espinoza-Seanez, 862 F.2d 526, 531 (5th Cir. 1988); United States v. Caicedo-Guarnizo, 723 F.2d 1420, 1421, 1423 (9th Cir. 1984) (holding search was valid under the extended border search doctrine despite the fact that it occurred several hours and over one-thousand miles from the defendant's border crossing).

[65] United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

[66] *Id.* at 155.

[67] *Id.* at 151 (reversing United States v. Molina-Tarazon, 279 F.3d 709 (9th Cir. 2002)).

[68] *Id.* at 150. "The terms 'port' and 'port of entry' refer to any place designated by Executive Order of the President, by order of the Secretary of the

part of a secondary inspection, CBP disassembled the vehicle's fuel tank where officers found more than eighty-one pounds of marijuana.[69] The Court emphasized that the dignity and privacy interests that mandate a certain level of suspicion to legitimate the search of one's person are not implicated in the search of a car.[70] The Ninth Circuit has affirmed that the routine/non-routine characterization is inapplicable to the inspection of objects, and is generally an issue only when the search is invasive to one's person.[71] Currently, the search of an object violates the Fourth Amendment only if the inspection was conducted in a "particularly offensive manner."[72] This standard permits Customs officials to thoroughly examine and even physically alter the object's composition, so long as the search is not unnecessarily destructive.[73]

III. COMPUTERS AND DISKETTES ARE SEARCHABLE CARGO

The *Flores-Montano* standard distinguishing the search of objects from that of people is critical to expand CBP's authority to examine laptop computers and diskettes. Current case law supports the ability of Customs to perform not only a superficial search (ensuring the device itself is not a threat) but also to conduct a closer inspection during which an agent may

---

Treasury, or by Act of Congress, at which a Customs officer is authorized to . . . collect duties, and to enforce the various provisions of the Customs and navigation laws." *See* 19 C.F.R. § 101.1 (2006).

[69] *Flores-Montano*, 541 U.S. at 150-51.

[70] *Id.* at 152. *See also* Tabbaa v. Chertoff, No. 05-CV-582S, 2005 WL 3531828, at *11 (W.D.N.Y. Dec. 22, 2005) (explaining that routine, suspicionless searches include stops to examine "personal effects").

[71] United States v. Chaudhry, 424 F.3d 1051, 1054 (9th Cir. 2005) (explaining that the Supreme Court in *Flores-Montano* specifically limited the distinction between "routine" and "non-routine" searches to those of one's person).

[72] *Flores-Montano*, 541 U.S. at 154 n.2 (quoting United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977)).

[73] *Id.* at 156 ("[W]e conclude that the Government's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank. While it may be true that some searches of property as so destructive as to require a different result, this was not one of them."). In *Chaudhry*, the Ninth Circuit similarly held that the drilling of a 5/16 inch hole in the bed of a pickup truck was not destructive enough to characterize the border search as non-routine. 424 F.3d at 1053 (citing *Flores-Montano*, 541 U.S. at 156). The court did leave open the possibility that a border search of an object might be so destructive as to require reasonable suspicion but declined to express an opinion regarding what that threshold might be. *Id.* at 1054.

browse material stored in the computer's hard drive or view the contents of accompanying disks.[74]

In *United States v. Irving*, a district court denied a defendant's motion to suppress evidence retrieved from computer diskettes during a border search; this denial was affirmed by the Second Circuit.[75] Although the Circuit Court declined to address whether or not the search of the diskettes was routine, the Court found no error with the district court's determination of the issue.[76] In May of 1998, Stefan Irving arrived at the Dallas-Fort Worth Airport on a flight from Mexico City.[77] He was questioned by Customs officials who proceeded to inspect his luggage, develop a roll of film, and view the contents of several computer diskettes.[78] The items contained numerous images of child pornography.[79] The Second Circuit affirmed the defendant's convictions under federal law,[80] as well as the denial of Irving's motion to suppress the evidence obtained during the airport search.[81] The Circuit Court determined that the CBP officers in this particular situation were acting under a reasonable suspicion.[82]

---

[74] *See* 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. Roberts, 86 F. Supp. 2d 678, 688 (S.D. Tex. 2000) (denying defendant's motion to suppress evidence retrieved from his computer during an outbound border search; although in this case defendant consented to the search, the inspection of his "computer would have been a routine export search, valid under the Fourth Amendment").

[75] *Irving*, 452 F.3d at 122-23.

[76] *Id.* at 123-24. *See also* United States v. Irving, No. S3 03 CR.0633(LAK), 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003) (explaining that since personal computers may be equated with closed containers, "the agents were entitled to inspect the contents of the diskettes even absent reasonable suspicion"), *reh'g granted*, 452 F.3d 110 (2d Cir. 2006).

[77] *Irving*, 452 F.3d at 115.

[78] *Id.*

[79] *Id.* Stefan Irving was "a former chief pediatrician for the Middletown, New York School district." *Id.* at 114. His license was revoked after he was convicted of attempted sexual abuse in the first degree of a minor. *Id.* Thirteen years later, Irving became the target as part of a "nationwide investigation of individuals suspected of traveling to Mexico for the purpose of engaging in sexual acts with children." *Id.* Irving was stopped when he was traveling home from a visit to the Castillo Vista del Mar in Acapulco, Mexico, "a guest house that served as a place where men from the United States could have sexual relations with [young] boys." *Irving*, 452 F.3d at 114.

[80] *Id.* Irving was convicted of unlawfully traveling outside of the United States for the purpose of engaging in sexual relations with minors in violation of 18 U.S.C. §§ 2241(c), 2423(b) (2000), and receiving and possessing pornographic images of children in violation of 18 U.S.C. § 2252A(a)(2)(B), (a)(5)(B). *Id.*

[81] *Id.* at 122-23.

[82] *Id.* at 124. Irving was a convicted pedophile; he had traveled to Mexico to visit what he called an "orphanage," and his luggage contained what appeared to be children's drawings. *Id.*

However, the significant portion of the opinion is that which fails to find error with the trial court's affirmation that the defendant's computer could be searched without suspicion.[83] The district court equated the device with an ordinary closed container or a locked piece of luggage for inspection purposes—the inspection of which "is the paradigmatic routine border search."[84]

The Fourth Circuit has explicitly affirmed CBP authority to inspect personal computers and view the contents of accompanying diskettes in *United States v. Ickes*.[85] Defendant John Ickes was stopped at the United States-Canada border for a routine inspection when Customs officials discovered drug paraphernalia and a photo album containing pornographic images of children.[86] CBP officers proceeded to examine Ickes's personal laptop computer as well as approximately seventy-five diskettes, all of which contained child pornography.[87] While the officers in this particular instance were operating under a reasonable suspicion triggered by the photo-album,[88] the court reiterated Customs' ability to search personal computers without such suspicion and emphasized the broad, statutory language from which CBP derives much of its authority.[89] Specifically, the court noted the

---

[83] *Id.*

[84] *See* United States v. Irving, No. S3 03 CR.0633(LAK), 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003) (quoting United States v. Roberts, 86 F. Supp. 2d 678, 689 (S.D. Tex. 2000)).

The trial court in *Irving* cited several cases supporting the "compar[ison of] personal notebook computers to closed containers for the purpose of the Fourth Amendment analysis." *Id. See also, e.g.*, United States v. Runyan, 275 F.3d 449, 458 (5th Cir. 2001) (assuming that computer disks are containers and that standards governing closed container searches apply); United States v. Al-Marri, 203 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) ("Courts have uniformly agreed that computers should be treated as if they were closed containers."); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (finding that "the Fourth Amendment protection of closed computer files and hard drives is similar to the protection it affords a person's closed containers and closed personal effects").

The *Irving* court concluded that the "agents were entitled to inspect the contents of the diskettes even absent reasonable suspicion. . . . [A]ny other decision effectively would allow individuals to render graphic contraband . . . largely immune to border search simply by scanning images onto a computer disk before arriving at the border." *Irving*, 2003 WL 22127913, at *5.

[85] 393 F.3d 501, 505 (4th Cir. 2005).

[86] *Id.* at 502-03.

[87] *Id.* at 503.

[88] "[Ickes] told a U.S. Customs Inspector that he was returning from vacation. The inspector, however, was puzzled . . . because Ickes's van appeared to contain 'everything he owned.'" *Id.* at 502.

[89] *Id.* at 503-04 (quoting 19 U.S.C. § 1581(a) (2000)).

embracive term "cargo"[90] and the repeated use of "any."[91] A reading of the plain language combined with the historical pedigree of the government's plenary power at the border negated any statutory interpretation that would exclude electronic devices from the scope of Customs authority.[92] In denying Ickes's motion to suppress the evidence obtained during the search, the court flatly rejected the argument that computers and computer disks are excluded from the contemplated reach of 19 U.S.C. § 1581(a).[93] Congress clearly intended broad application of the statute and did not need to explicitly include electronic equipment.[94]

Perhaps even more importantly, the Fourth Circuit concluded that the personal, expressive nature of information capable of storage on a computer or disk is irrelevant to CBP's search authority.[95] The court noted the "staggering" ramifications for national security that would result from an exemption for electronic information, that such logic would create a sanctuary for terrorist plans which are inherently expressive.[96] Officers would also be faced with the impossible task of distinguishing personal files from non-expressive material, creating costly, time consuming legal dilemmas not meant to occur during a border search.[97] Creating an exception at the border for computer files would undermine the very

---

[90] "Cargo" means "goods transported by a vessel, airplane, or vehicle." BLACK'S LAW DICTIONARY 226 (8th ed. 2004).

[91] *See Ickes*, 393 F.3d at 504. The U.S.C. provides that:

> *Any* officer of the customs may at *any* time go on board of *any* vessel or vehicle at *any* place in the United States or within the customs waters or, as he may be authorized, within a customs-enforcement area . . . , or at *any* other authorized place . . . and examine . . . documents and papers and examine, inspect, and search . . . every part thereof and *any* person, trunk, package, or cargo on board . . . .

19 U.S.C. § 1581(a) (2000) (emphasis added). The language of the present statute is virtually identical to that of the customs statute passed by the first congress. *See supra* note 41.

[92] *Ickes*, 393 F.3d at 504-06. The court also relied on the Supreme Court's decision in *United States v. Flores-Montano*, 541 U.S. 149 (2004), as an indication that border search authority should be as broad as possible within constitutional bounds. *Ickes*, 383 F.3d at 505.

[93] *Ickes*, 383 F.3d at 504.

[94] *Id.*

[95] *Id.* at 506.

[96] *Id. See also* United States v. Irving, No. S3 03 CR.0633(LAK), 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003).

[97] *Ickes*, 383 F.3d at 506.

foundation of the border search doctrine and negate its effectiveness.[98]

The notion that a laptop computer is the equivalent of a closed-container for Fourth Amendment purposes would seem equally applicable to hand-held electronic devices and PDAs. PDAs and other hand-held wireless communication devices are nearly identical to laptops in both function and storage capacity.[99] Applying the *Flores-Montano* methodology to these objects, CBP clearly has the authority to examine the contents of such electronic "cargo" during a border inspection, regardless of the presence of an independent trigger providing reasonable suspicion.[100] Thus, according to present case law, the logical conclusion appears to be that CBP has authority to search a traveler's iPod, BlackBerry, Palm Pilot, or flash drive without reasonable suspicion.

IV. THE AUTHORITY TO PHOTOCOPY PAPER MATERIALS AT THE BORDER

Directly associated with CBP's authority to search all cargo crossing the border[101] is the government's ability to photocopy or reproduce material found during inspection.[102] Material replicated during a border search often proves to be critical evidence in a later criminal prosecution.[103] The authority to copy paper materials has been uniformly upheld since the 1985 Fifth Circuit decision in *United States v. Fortna*.[104] In *Fortna*, the court established that the photocopying of papers tending to prove the defendant's participation in a drug trafficking conspiracy was constitutionally valid.[105] *Fortna*'s progeny have continued to affirm the validity of this holding, demonstrated as recently as 2001 in the successful prosecution of one of Osama bin Laden's

---

[98] *Id.*

[99] *See infra* Part V.A.

[100] 19 U.S.C. § 1581(a) (2000).

[101] 19 U.S.C. § 482 (2000).

[102] *See, e.g.*, United States v. Fortna, 796 F.2d 724, 738-39 (5th Cir. 1986); United States v. Soto-Teran, 44 F. Supp. 2d 185 (E.D.N.Y. 1996), *aff'd*, 159 F.3d 1349 (2d Cir. 1998); State v. Codner, 696 So. 2d 806, 809 (Fla. Dist. Ct. App. 1997).

[103] United States v. Schoor, 597 F.2d 1303, 1306 (9th Cir.1979) ("[C]ustoms officials were themselves entitled to seize . . . documents, . . . having been notified that [the documents] were the instrumentalities of a crime involving the illegal importation of [narcotics].").

[104] 796 F.2d 724 (5th Cir. 1986).

[105] *Id.* at 738-39.

top aides.[106] Additionally, this authority has been held applicable to outbound packages not carried on one's person while traveling.[107] However, limitations on the ability to copy paper material have also been established.[108] Ultimately, *Fortna* and its progeny must be read in light of the recent circuit court decisions in *Irving* and *Ickes*. CBP must be allowed to not only search electronic devices but also to copy electronic material stored therein, subjecting only the reproduction of digital evidence to a reasonable suspicion standard.

A. United States v. Fortna

In *Fortna*, the Fifth Circuit held, *inter alia*, that Customs officers may photocopy what they believe to be incriminating evidence during a validly executed border inspection.[109] On April 15, 1985, George Sharer arrived at the Dallas-Fort Worth International Airport on a flight from Mexico City.[110] Customs officials found several documents of interest in his carry-on luggage which they proceeded to read closely and photocopy.[111] These documents included a map of northern Mexico indicating airstrip locations, two airline tickets to Bogotá, Colombia, and a note that read "'Pick up pilot in Miami.'"[112] Sharer and three other men were later convicted of conspiracy to import cocaine.[113] The Fifth Circuit denied Sharer's motion to suppress the evidence photocopied during the airport inspection.[114] The court first stated that "[t]he search [of] Sharer's personal belongings . . . was clearly justified because he was crossing [the United States] border."[115] The court further explained that since Sharer could have no legitimate expectation of privacy in this context, he could not reasonably believe that his documents could be shielded from

---

[106] *See* discussion *supra* Part I.

[107] *See* United States v. Seljan, 328 F. Supp. 2d 1077, 1078-81 (C.D. Cal. 2004).

[108] *See, e.g.*, People v. LePera, 611 N.Y.S.2d 394, 396 (App. Div. 1994).

[109] *Fortna*, 796 F.2d at 738-39.

[110] *Id.* at 738.

[111] *Id.*

[112] *Id.* The originals were promptly returned to the travelers. *Id.*

[113] *Id.* at 727.

[114] *Id.* at 739.

[115] *Fortna*, 796 F.2d at 738.

customs officials during inspection.[116] Nothing more was needed to justify the photocopying of the materials.[117] The reproduction of the evidence "merely memorialized the agents' observations and provided a means to verify any subsequent recounting of them."[118] The Fifth Circuit concluded that as long as the initial inspection is valid and the photocopying is done in "good faith" and to further a "legitimate governmental purpose[]," no constitutional rights are violated.[119]

The authority to copy paper at the border has been consistently upheld.[120] In *United States v. Soto-Teran*, the Eastern District Court of New York adhered to the holding of *Fortna* and rejected a claim that the reproduction of a personal letter by Customs violated the privacy rights of both the letter's carrier and the addressee.[121] Defendant Nelson Soto-Teran was stopped by the Customs Service for a routine inspection after he arrived at the Miami International Airport on a flight from Cali, Colombia.[122] During questioning, Soto appeared nervous; his "hands were shaking, sweat appeared on his brow, and he would not make eye contact."[123] Officers proceeded to take Soto to a secondary inspection area where they found a sealed letter in his briefcase, which they carefully read and photocopied.[124] After returning the letter, the officers searched Soto's wallet and telephone book, copying various pieces of paper indicating involvement in narcotics smuggling.[125] Less than one month later, Soto was arrested and indicted on substantive charges relating to the mass importation and distribution of cocaine.[126]

---

[116] *Id.*

[117] *See id.*

[118] *Id.*

[119] *Id.* at 738-39.

[120] *See* United States v. Bin Laden, No. S(7) 98 CR. 1023, 2001 WL 30061, at *4 (S.D.N.Y. Jan. 2, 2001) ("The mere fact that the Government photocopied the Defendant's papers does not make the search unreasonable in scope."). *See also* United States v. Ramos, Nos. 93-50416, 93-50531, 93-50546 and 93-50559, 1995 WL 89427, at *1 (9th Cir. Mar. 2, 1995) (denying motion to suppress photocopy of defendant's date book in prosecution for conspiracy to traffic cocaine; search was valid and nothing unreasonable about the copying); State v. Codner, 696 So. 2d 806, 810-11 (Fla. Dist. Ct. App. 1997) (holding photocopying of contents of defendant's wallet reasonable during valid, routine border search).

[121] United States v. Soto-Teran, 44 F. Supp. 2d 185, 191-92 (E.D.N.Y. 1996), *aff'd*, 159 F.3d 1349 (2d Cir. 1998).

[122] *Id.* at 188.

[123] *Id.*

[124] *Id.* at 188-89.

[125] *Id.* at 189.

[126] *Id.* at 187, 189.

His motion to suppress the photocopied evidence obtained during the border search was denied.[127] The court described the "unlimited discretion" of customs officials to search packages and the necessarily broad authority to inspect locked luggage and personal belongings.[128] The court concluded that a reasonable suspicion standard[129] should apply when CBP officers photocopy personal documents.[130] In rejecting the argument of the letter's addressee that her First Amendment rights were violated, the court emphasized the fact that neither a letter's carrier nor addressee may legitimately expect privacy at the border.[131] Based on the holdings of *Fortna* and *Soto-Teran*, the photocopying of materials during a border search is clearly permissible and requires nothing more than reasonable suspicion. This authority violates neither the Fourth Amendment's protections nor the privacy interests of travelers.

CBP officers' ability to inspect and photocopy personal documents also applies to material entering and exiting the country via commercial carriers.[132] In *United States v. Seljan*, a district court denied a motion to suppress evidence copied during the search of three outbound FedEx packages at the international border's functional equivalent.[133] In *Seljan*, the defendant was suspected of using an interstate facility to entice a minor by sending sexually explicit material to an eight year old girl in the Philippines.[134] First, the district court determined that the officers were acting under statutory authority to interdict the export of unreported currency when they opened the first FedEx package.[135] Upon opening the first package and discovering evidence indicating the defendant's sexual involvement with a child, the officers were acting under

---

[127] *Soto-Teran*, 44 F. Supp. 2d at 187 (citations omitted).

[128] *Id.* at 190-91.

[129] Factors giving rise to reasonable suspicion included the suspect's excessive nervousness and origination of flight from Colombia, a known source country for drugs. *Id.* at 188. *See also* United States v. Charleus, 871 F.2d 265, 269 (2d Cir. 1989) (citing "whether the suspect's flight originated at a known source of drugs" as influencing the possibility of reasonable suspicion).

[130] *Soto-Teran*, 44 F. Supp. 2d at 1991.

[131] *Id.* at 192-93. The valid inspection did not "chill[]" addressee's First Amendment rights. *Id.* at 193. "[T]he Supreme Court [has] implicitly approved border searches of articles [and] containers." *Id.* (citing United States v. Ramsey, 431 U.S. 606, 623 (1977)).

[132] *See, e.g.*, United States v. Seljan, 328 F. Supp. 2d 1077 (C.D. Cal. 2004).

[133] *Id.* at 1086.

[134] *Id.* at 1084. *See* 18 U.S.C. § 2422(b) (2000) (prohibiting the use of an interstate facility to entice a minor).

[135] *Seljan*, 328 F. Supp. 2d at 1079 (citing 31 U.S.C. § 5316 (2000)).

reasonable suspicion when they opened the following two packages and photocopied their contents.[136] The court concluded that CBP officials properly acted in furtherance of a legitimate government purpose: the preservation of evidence.[137]

B. Limits on the Scope of Fortna

The ability to photocopy or reproduce information found during a border search is not absolute. This authority is subject to several limitations regarding the scope of CBP law enforcement as well as the ability to retain and disseminate personal information.[138] While CBP is responsible for the collection of duties,[139] the Agency must also enforce over four hundred laws on behalf of forty federal agencies—namely restrictions designed to protect Americans from dangerous and illegal goods.[140] Despite this immense responsibility, CBP officers are nonetheless restricted and do not possess the general investigative or enforcement authority of state police.[141] In *People v. LePera*, a New York court emphasized this point by suppressing photocopied gambling records obtained during a search at the United States-Canada border.[142] The court clarified that while the search of the defendant's vehicle and subsequent photocopying of his papers would be valid if officers suspected a violation of federal gambling laws,[143] the same could not hold true for the commission of an offense defined only in the New York Penal Code.[144] The court emphasized that

---

[136] *Id.* at 1084. In the first of the three Federal Express packages searched by Customs, letters were found in which defendant requested pictures of the girl. *Id.* Officers has reason to suspect that defendant was violating 18 U.S.C. § 2422(b), and therefore, the search of the other two packages was proper. *Id.*

[137] *Id.* at 1085. *Cf.* United States v. Cardona, 769 F.2d 625, 629-30 (9th Cir. 1985) (holding that Customs official could present evidence regarding his observations, but the photocopies obtained during inspection must be suppressed, since the contents of the FedEx package were not subject to seizure).

[138] *See generally* Heidy v. U.S. Customs Serv., 681 F. Supp. 1445 (C.D. Cal. 1988); People v. LePera, 611 N.Y.S.2d 394 (App. Div. 1994).

[139] CBP collects more than $81 million dollars in revenue each day. *See* CPB, A Day in the Life of U.S. Customs and Border Protection, http://www.cbp.gov/xp/cgov/toolbox/about/accomplish/day.xml [hereinafter CPB, A Day in the Life] (last visited Sept. 15, 2006).

[140] *See* CBP, CBP Cargo Examinations, http://cbp.gov/xp/cgov/border_security/port_activities/cargo_exmainations.xml (last visited Sept. 13, 2006).

[141] *LePera*, 611 N.Y.S.2d at 397.

[142] *Id.* at 397-98. New York State makes the possession of gambling records a crime. N.Y. PENAL LAW § 225.20 (McKinney 2000).

[143] *See* 18 U.S.C. § 1955 (2000) (prohibiting illegal gambling businesses).

[144] *LePera*, 611 N.Y.S.2d at 397-98.

federal regulations explicitly limit CBP by confining property seizures to situations in which a "Customs officer . . . believe[s] *that any law or regulation enforced by the Customs Service* has been violated."[145]

Additionally, courts have limited the Bureau's ability to retain and share photocopied evidence with other law enforcement agencies.[146] In *Heidy v. United States Customs Service*, a district court in California announced that a Customs practice of keeping photocopied evidence and records of non-violation of federal law was constitutionally impermissible.[147] The plaintiffs in *Heidy* were United States citizens re-entering the country from Nicaragua.[148] During inspection, Customs officials searched and photocopied all papers carried by the individuals to ensure that the travelers were not importing seditious material.[149] With the Federal Bureau of Investigation's (FBI) assistance, Customs made permanent records consisting of the identity of each person from whom material was seized and a final determination regarding the legality of the documents.[150] Although the written material was found not to violate federal law, the copies and records were nonetheless retained by both Customs and the FBI.[151] The individuals feared that government's possession of these records would subject them to future inquiries upon reentry.[152] The court acknowledged Customs authority to review and copy written material during a border search, but ordered the destruction of records of non-violation.[153] Specifically, the Service was to: (1) return any originals to the owner, (2) destroy all copies and records reflecting individual identity, and (3) refuse dissemination to any federal agency not willing to comply with Customs policies.[154]

---

[145] *Id.* at 397 (quoting 19 C.F.R. § 162.21(a) (2006)).

[146] *See* Heidy v. U.S. Customs Serv., 681 F. Supp. 1445, 1453 (C.D. Cal. 1988).

[147] *Id.*

[148] *Id.* at 1446.

[149] *Id.* at 1446-47. CBP is charged with enforcing the law prohibiting persons from "importing into the United States from any foreign country any book, pamphlet, paper, [or] writing . . . containing any matter advocating or urging treason or insurrection against the United States or forcible resistance to any law of the United States." 19 U.S.C. § 1305(a) (2000).

[150] *Heidy*, 681 F. Supp. at 1446-47.

[151] *Id.* at 1447.

[152] *Id.* at 1448.

[153] *Id.* at 1448, 1453.

[154] *Id.* at 1453.

While CBP maintains broad authority under the border search doctrine to examine and photocopy materials found during inspection, this authority is limited. The limits regarding Customs enforcement power and the retention of copied evidence are adequate protections for those traveling across the United States border with paper documents. These protections are equally effective in the digital context. Thus, CBP must be able to reproduce electronic information under the same principles established in *Fortna* and *Soto-Teran*.

C. Reproduction of Digital Information under the Fortna *Principle*

The authority established by *Fortna* and its progeny to copy written materials during a border inspection may logically be applied to digitally stored information as well. The authority to browse the contents of a traveler's PDA or laptop would be useless if CBP were unable to obtain a hard copy of incriminating files found therein. The ability to view but not to duplicate electronically stored files would allow travelers to delete material implicating involvement in a federal criminal offense during or moments after a search.

First, the Fourth Amendment's protections are inapplicable in the border search context.[155] Second, one must apply the new *Flores-Montano* method, since computers and hand-held electronic devices are inanimate objects, thus making the routine/non-routine distinction irrelevant.[156] CBP may examine these items as it would any other form of cargo, without reasonable suspicion. Finally, since there is no constitutional impediment to photocopying paper material examined during a search, the *Fortna* authority to reproduce evidence must be applied to electronic information as well. The reproduction of all digitally stored information must be permitted when reasonable suspicion is present. While the medium has changed, the logic has not. Electronically stored documents should receive no more protection than material in the analog world.

---

[155] *See supra* Part II.A.

[156] *See supra* Part II.C.

V. THE NEED TO APPLY *FORTNA* TO DIGITAL INFORMATION

The application of the border search exception and the principle of *Fortna* to electronic devices and the digital information contained therein is vital to the protection of our nation and the integrity of our border. Customs officials must be able to search all laptops and PDAs that enter the U.S. and reproduce information contained therein, memorializing their observations should subsequent verification of them prove necessary in a criminal prosecution.[157] Portable electronic devices, laptop computers, and disks are unique in both the quantity and nature of personal information these objects may contain. However, one may not reasonably entertain an expectation of privacy while crossing the international border.[158] While travelers may disapprove of the government's authority to browse vast amounts of personal communications and emails, the consequences of creating an exemption for such material far outweigh individual privacy concerns. Creating a sanctuary at the border for digital information would cripple Customs in the fight against terrorism, narcotics trafficking, illegal money transfers, and child pornographers. Existing protections and the adoption of a new CBP policy providing for the destruction of copied materials are adequate safeguards.

A. The Unique Obstacle Presented by Digital Information

> We are in the midst of an information revolution . . . . Digital technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who we are and what we own . . . small details . . . are now preserved forever in the digital minds of computers.[159]

Laptop computers, PDAs, flash drives, and myriad other hand-held devices that have proliferated in recent years present a unique security obstacle for CBP as well as privacy concerns for the international traveler. The mobile electronics market has grown dramatically in the last decade and the storage capacity of these machines presents issues not previously encountered in the border search context. Typically, the amount of personal belongings and paper documents an individual may carry while traveling is limited by both space

---

[157] *See* United States v. Fortna, 796 F.2d 724, 738 (5th Cir. 1986).

[158] *See supra* Part V.B.

[159] DANIEL SOLOVE, THE DIGITAL PERSON 1 (2004).

and weight considerations.[160] However, computer hard drives and PDAs present their owners with the opportunity to carry more information in their carry-on luggage than one might contemplate transporting in analog form. For example, computer hard drives sold in 2005 have a storage capacity of around eighty gigabytes.[161] This is "roughly equivalent to forty million pages of text - about the amount of information contained in the books on one floor of a typical academic library."[162] As computers become smaller, lighter, and generally more compact, travelers may be able to carry nearly sixty gigabytes of hard drive space on a machine weighing less than three pounds.[163] In addition, USB flash drives, the modern equivalent of floppy disks, are typically no larger than a stick of gum and may contain up to two gigabytes of storage, maintaining data for nearly ten years.[164]

While PDAs are not equipped with the same vast amount of storage space, they come close. The BlackBerry,[165] one of the most popular wireless communication devices on the market, comes equipped with anywhere from sixteen to sixty-four megabytes of storage depending on the model.[166] Assuming

---

[160] Generally, travelers are limited to two pieces of luggage which must be checked and can weigh anywhere from fifty to seventy pounds depending on class and the destination of the flight; one carry-on item is typically allowed but is not to exceed forty pounds in weight. *See* American Airlines, Baggage Allowance, http://www.aa.com/content/travelInformation/baggage/baggageAllowance.jhtml (last visited Aug. 28, 2006); Delta Skyteam, Baggage Allowance on Flights, http://www.delta.com/traveling_checkin/baggage/baggage_allowance/index.jsp (last visited Aug. 28, 2006); US Airways, Baggage Policies, http://www.usairways.com/awa/content/traveltools/baggage/baggagepolicies.aspx (last visited Aug. 31, 2006).

[161] A gigabyte is "[a] unit of information equal to one billion . . . bytes or one thousand megabytes." Webster's Online Dictionary, Gigabyte, http://www.websters-online-dictionary.org/definition/gigabyte (last visited Sept. 13, 2006). A byte holds the equivalent of a single character, such as a letter, dollar sign, or decimal point. Webster's Online Dictionary, Byte, http://www.websters-online-dictionary.org/definition/byte (last visited Aug. 28, 2006).

[162] *See* Kerr, *supra* note 30, at 542. The amount of storage space available on computer hard drives "tend[s] to double about every two years." *Id.*

[163] The Sony VAIO TX series offers models with such storage capacity and weight. Sony, http://www.sonystyle.com (follow "Computers: Notebooks" hyperlink; then follow "TX Series" hyperlink) (last visited Aug. 28, 2006).

[164] USB Flash Drive Alliance, USB Flash Drive Overview, http://www.usbflashdrive.org/usbfd_overview.html (last visited Aug. 28, 2006).

[165] The BlackBerry is manufactured by Canadian company Research in Motion. *See* Research in Motion Homepage, http://www.rim.com (last visited Sept. 13, 2006).

[166] For example, the 7280 model contains sixteen megabytes of memory while the new Pearl 8100 model contains sixty-four and accepts micoSD cards that are capable of expanding that capacity. *See* BlackBerry, http://www.discoverblackberry.com/devices/ (last visited Oct. 4, 2006).

all of that space was used for text communications, a sixty-four-megabyte BlackBerry would theoretically permit a traveler to carry the equivalent of 32,000 pages of text, sixty-four thick books, or over 60,000 emails in their purse or coat pocket.[167] These machines generally include a personal organizer containing an address book, calendar, memo pad, and task list, as well as Yahoo! Instant Messenger.[168] Apple Computer's ubiquitous iPod is also growing in terms of memory and storage capacity.[169] Software enhancements make the digital music player more akin to a PDA since the device may also be used as an external hard drive for the backup and transportation of files.[170] As of September 2006, the most recent version of the iPod can accommodate videos, 25,000 personal photos, and contains a calendar and address book.[171] In addition to information intentionally downloaded or entered onto the device by the user, many operating systems and programs store information about how and when the device has been used, including information about the user's interest, habits, and online activity—all of this unknown to the user himself.[172]

Clearly the international traveler of the twenty-first century has the ability to carry a warehouse of personal information in a comparatively miniscule amount of space.[173] This, however, is not reason to restrict CBP's authority but

---

[167] One megabyte is equal to 1,024 kilobytes. One kilobyte is equivalent to one half page of text, the size of an average email without an attachment. *See* wiseGEEK, How Much Text is in a Kilobyte or Megabyte?, http://www.wisegeek.com/how-much-text-is-in-a-kilobyte-or-megabyte.htm (last visited Aug. 28, 2006).

[168] *See* BlackBerry, BlackBerry Desktop Software, http://www.blackberry.com/products/software/desktop/index.shtml (last visited Aug. 31, 2006). Hewlett Packard's popular iPAQ offers similar features and storage space. *See* Hewlett Packard, Introduction to Handheld PC's, http://h71036.www7.hp.com/ hho/cache/9044-0-0-225-121.aspx (last visited Jul. 31, 2006).

[169] *See* Apple, iPod, http://www.apple.com/ipod/ipod.html (last visited Sept. 1, 2006).

[170] David Pogue, *State of the Art; Online Piper, Payable by the Tune*, N.Y. TIMES, May 1, 2003, at G1.

[171] *See* Apple, iPod, http://www.apple.com/ipod/ipod.html (last visited Sept. 1, 2006).

[172] Kerr, *supra* note 30, at 542-43. Word processing programs such as Microsoft Word create "temporary files that permit analysts to reconstruct the development of a file," while internet browsers create a cache of web pages visited so that both the user's browsing history and the actual search terms entered into an engine, such as Google, may be retrieved. *Id.* at 543.

[173] A BlackBerry weighs less than five ounces. BlackBerry, Compare Devices, http://www.blackberry.com/compare/compare.do?handhelds=81&handhelds=202&handhelds=242&handhelds=243&handhelds=101&method=getFeatureView&x=51&y=14 (last visited Sept. 13, 2006).

reason to expand it. The storage capabilities of electronic devices and the vast quantity of information such machines may contain demand this result.[174] The advent of new technology and the increased digitalization of personal information presents CBP with a unique obstacle in the inspection and reproduction of potentially valuable evidence. Admittedly, the amount of information that may be stored on these devices is a legitimate concern for travelers and merits a consideration the role of the Fourth Amendment, its protection of a person's "papers," and implicit constitutional protections of information privacy.[175] However, the following sections will demonstrate that the absence of reasonable expectations of privacy at the border combined with the practical consequences of allowing such an exemption for electronic data demand the application of *Fortna* to current technology. The preservation of electronic evidence is necessary for the efficient protection of our borders and the enforcement of federal law. Existing protections established under *Fortna* and its progeny combined with a policy of non-retention and non-dissemination is enough to preserve the interests of those crossing the border.

B. Information Privacy Concerns are Inapplicable at the Border

Although absent from the text of the Constitution and lacking a uniform definition, privacy may be interpreted as the control over information about ourselves and its communication to others.[176] In *Griswold v. Connecticut*, the Supreme Court identified an implicit constitutional right to privacy.[177] The Court invalidated a Connecticut law banning the use of contraceptives and identified zones in which the confidential relationships of citizens are protected from governmental intrusion.[178] Later, this definition was expanded to encompass information privacy as well.[179] The Supreme

---

[174] *See* United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005).

[175] *See* Adams, *supra* note 18, at 371.

[176] *See* Alan Westin, *Privacy and Freedom*, *in* DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 28, 28 (2003).

[177] 381 U.S. 479, 485 (1965).

[178] *Id.* at 485. *See also* SOLOVE, *supra* note 159, at 64.

[179] Whalen v. Roe, 429 U.S. 589, 599 (1977) (upholding New York state law requiring records to be kept of prescriptions involving addictive substances but identifying information privacy as a constitutionally protected). *See also* SOLOVE, *supra* note 159, at 65.

Court identified "the individual interest in avoiding disclosure of personal matters" as constitutionally protected.[180] It is this interest in avoiding the disclosure of personal information that is implicated in the border search of electronic devices and the reproduction of digital information.[181]

The Supreme Court has interpreted the Constitution to protect personal information from disclosure; however, the expectation of that privacy is neither reasonable nor applicable at the border.[182] In his concurring opinion in *Katz v. United States*, Justice Harlan explained the notion of a reasonable expectation of privacy and set forth a two-part inquiry to guide Fourth Amendment analyses for determining the validity of a search.[183] The first question is whether the individual manifested a subjective expectation of privacy in the object of the challenged search.[184] The second inquiry is whether society is willing to recognize that privacy expectation as reasonable.[185] While it remains true that the Fourth Amendment protects people and not places, the amount of privacy afforded and that which may reasonably be expected inevitably depends on place.[186] While privacy expectations at home are correctly at their highest, the same does not hold true at the border, where one may not reasonably expect to be free from unwarranted searches and seizures.[187] Thus to be protected under the two-

---

[180] *Whalen*, 429 U.S. at 599-600 (footnote omitted).

[181] Information privacy seems to be "implicit in the Fourth Amendment's [specific] protection of personal 'papers.'" Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 288 (2003).

[182] United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004) (discussing lack of expectation of privacy of property at United States border); United States v. Ramsey, 431 U.S. 606, 623 n.17 (1977) (same).

[183] 389 U.S. 347, 360 (1967) (Harlan, J., concurring). *See also* 1 JOHN WESLEY HALL, SEARCH AND SEIZURE 58-59 (3d ed. 2000).

[184] *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

[185] *Id.* (Harlan, J., concurring).

[186] *Id.* at 351*; see also* INFORMATION PRIVACY LAW, *supra* note 176, at 585.

[187] For cases upholding the highest expectation of privacy in the home, see Stanley v. Georgia, 394 U.S. 557, 568 (1969) (holding that although "the States retain broad power to regulate obscenity; that power simply does not extend to mere possession by the individual in the privacy of his own home"); Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

For cases illustrating the lowered expectations at the border, see United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985); Carroll v. United States 267 U.S. 132, 134-35 (1925) (upholding constitutionality of search and seizure of defendant's vehicle; affirming conviction for violation of the National Prohibition Act). "Customs officers are granted power by Congress to search persons and property . . . . [This authority] may be said to be a right which the Government

pronged *Katz* test, an individual must (1) "exhibit an actual (subjective) expectation of privacy" in his or her laptop or PDA, and (2) "that expectation [must] be one that society is prepared to recognize as 'reasonable.'"[188] In the context of the United States border, the inquiry fails. "[A] port of entry is not a traveler's home;" expectations of privacy are significantly lessened when balanced with the government's compelling interests at the border.[189]

Privacy is in constant tension with security interests and law enforcement's ability to prevent criminal activity.[190] However, "[t]he . . . line between an [impermissible] search . . . and an appropriate law enforcement practice [clearly depends on] a person['s] . . . reasonable expectation of privacy in the object of the search."[191] The compelling security interests in the border context far outweigh the information privacy interests a traveler may reasonably expect to have,[192] especially in the context of personal objects.[193] Privacy expectations for the information contained in electronic devices are simply unreasonable and the consequences of such immunity would be enormous.

C. Consequences of an Exemption for Electronic Devices

Establishing immunity for digital information at the border would result in a federal agency unable to adapt to modern methods of criminal evasion, thus rendering the enforcement powers of CBP meaningless. Such an exception would prevent the effective policing of our borders with the most striking consequences evident in the battle against terror, drugs, the illegal flow of money, and the protection of minors from sexual exploitation.

---

exercises over individuals in exchange for the privilege of entering the territory of the United States." *Id.*

[188] *Katz*, 389 U.S. at 361 (Harlan, J., concurring); HALL, *supra* note 183, at 58-59.

[189] United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971) (explaining that one's "right to be let alone" prevents neither the search of luggage nor the seizure of illegal materials when possession of them is discovered during such a search).

[190] INFORMATION PRIVACY LAW, *supra* note 176, at 275.

[191] *See* 2 HALL, *supra* note 183, at 426 (citing Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

[192] *See* discussion *supra* Part II.

[193] *See generally* United States v. Flores-Montano, 541 U.S. 149 (2004).

As the Fourth Circuit emphasizes in *United States v. Ickes*, the national security ramifications of an exemption for digital information would be "staggering."[194] Efforts to prevent another terrorist attack on United States soil have been dubbed the War on Terror.[195] This offensive has been launched against an elusive, amorphous target with a scale of activity unlike anything previously seen.[196] The fight against terrorism at the border proves to be one of the government's toughest obstacles. For example, CBP seizing over ninety percent of contraband in the form of controlled substances or child pornography would be considered an unparalleled law enforcement success.[197] The same line of thinking does not apply in the context of terrorism.[198] Allowing less than "10 percent of terrorists or materials for major terrorist acts" across the border could result in a catastrophic national disaster.[199] Customs must not only prevent the physical entry of lethal toxins and infectious agents but also intercept terrorist communications and uncover plans and conspiracies prior to an attack.[200] Immunity for electronically stored information from search and replication would create an enormous loophole for individuals planning an attack on U.S. nationals.

The assumption that al Qaeda does not use e-mail has been deemed erroneous by the FBI.[201] The fact has been established that terrorists use information technology for a variety of purposes, including the planning of attacks, fund raising, communication, and the dissemination of propaganda.[202] As the rest of the world has turned to laptops and wireless communication devices for the storage of personal information, it appears terrorists have as well. During the

---

[194] 393 F.3d 501, 506 (4th Cir. 2005).

[195] Jonathan P. Caulkins et al., *Lessons of the "War" on Drugs for the "War" on Terrorism*, *in* COUNTERING TERRORISM 73, 73 (Arnold M. Howitt & Robyn L. Pangi eds., 2003).

[196] *Id.* at 73-74.

[197] *Id.* at 83-84.

[198] *Id.*

[199] *Id.*

[200] *Id.* at 75, 83.

[201] Elsa Walsh, *Learning to Spy; Can Maureen Baginski Save the F.B.I.?*, THE NEW YORKER, Nov. 8, 2004, at 96.

[202] Michael A. Vatis, *Cyber Attacks: Protecting America's Security Against Digital Threats*, *in* COUNTERING TERRORISM, *supra* note 195, at 219, 229 (citing Testimony of FBI Director Louis J. Freeh, Before the Senate Select Committee on Intelligence, May 10, 2001, http://www.fbi.gov/congress/congress01/freeh051001.htm).

investigation of the 1993 World Trade Center bombing in New York, officials found detailed plans to destroy U.S. bound airliners in encrypted files on the suicide bomber's laptop.[203] In 2004, a raid on a home in Pakistan uncovered a "'treasure trove' of information" contained on laptop computers and disks indicating al Qaeda's resolve to commit more attacks on United States soil.[204] As the court in *Ickes* reminds us—this type of material is inherently personal and expressive. [205] However, creating a sanctuary for such communications because of privacy concerns would undermine the compelling reasons that lie at the heart of the border search doctrine.[206] Failure to apply the border search doctrine and the *Fortna* holding to the digital medium would cripple "America's frontline"[207] in the war on terror.

The impact would be equally enormous on America's other prominent battle, the War on Drugs.[208] The seizure of controlled substances accounts for a large portion of CBP activity.[209] The ability of Customs to effectively counter the inbound flow of narcotics depends on the government's authority to search not only for physical contraband but for

---

[203] *Id.*

[204] *Al-Qaeda in America: The Terror Plot*, TIME, Aug. 16, 2004, at 28. On July 24, 2004, a raid on the Pakistani home of an al Qaeda leader "uncovered three laptop[s] . . . and 51 . . . discs" containing "500 photographs of potential targets inside the U.S., . . . detailed analyses of the vulnerabilities to a terrorist attack of several of them and communications among some of the most wanted terrorists in the world. . . . [T]he surveillance data on the hard drives [was] at least three years old." *Id.*

[205] *See* United States v. Ickes, 393 F.3d 501, 506 (4th Cir. 2005).

[206] *Id.*

[207] CBP, CBP Mission Statement and Core Values, http://customs.gov/xp/cgov/toolbox/about/mission/guardians.xml (last visited Sept. 14, 2006).

[208] Laurie L. Levenson, *Border Searches*, 26 NAT'L L.J. 7, 8 (2004). It is illegal "to import to or export from the United States any controlled substance or narcotic drug listed in schedules I through V of the Controlled Substances Act . . . ." 19 C.F.R. § 162.61 (2006). Controlled substances prohibited by Schedules I through V include: cocaine, heroin and other opiate derivatives, marijuana, methamphetamine, morphine, and peyote. 21 U.S.C. § 812(c) (2000).

In the early 1970s, President Richard Nixon declared a war on drugs and called for an aggressive attack on the country's "public enemy number one." STEVEN WISOTSKY, BREAKING THE IMPASSE IN THE WAR ON DRUGS 3 (1986) (citing EDWARD J. EPSTEIN, AGENCY OF FEAR 178 (1977)). Nixon created the Drug Enforcement Administration ("DEA") and greatly expanded the federal government's involvement in the effort to disrupt the importation of controlled substances across our border. *Id.* at 249-51.

[209] During the 2005 federal fiscal year, Customs "officers seized over 127 tons of narcotics at Southern California ports of entry alone." News Release, CBP, CBP Sees Increase in Drug and Migrant Interceptions in California (Jan. 24, 2006) http://www.cbp.gov/xp/cgov/newsroom/news_releases/012006/01242006.xml (last visited Sept. 14, 2006).

evidence of trafficking conspiracies as well.[210] *Fortna* provides a classic example of the type of evidence that must be obtained and reproduced for use in criminal prosecutions.[211] As terrorists have turned to computer storage, there is no reason to believe that narco-traffickers would not do the same. Uploading maps, travel itineraries, and personal communications to a BlackBerry would be far safer and more efficient than carrying the same information in the bulkier, more readily searchable paper form.[212] Digital information is also easier to delete moments before a Customs inspection. Under *Ickes* and *Irving*, CBP would be able to view this information but not reproduce it. *Fortna* must be extended to resolve this problem. Officers must be permitted to memorialize their observations and provide a means to verify a subsequent recounting of them, thus preventing traffickers from destroying incriminating evidence with the push of a button.[213] Exempting electronic data from replication or, alternatively, requiring a higher standard of suspicion for reproduction, would prevent Customs from obtaining evidence needed to convict those trafficking in deadly narcotics for personal profit.[214]

Immunity from search and reproduction for electronic information would also prevent CBP from stemming the illegal cross-border transfer of money used to fund terrorist organizations and drug cartels and to launder tainted proceeds.[215] Customs must not only prevent the flow of illegal contraband and watch for terrorist communications, but the Agency is also responsible for monitoring the illegal flow of

---

[210] *See* United States v. Fortna, 796 F.2d 724, 738 (5th Cir. 1986).

[211] *Id.* at 738-39.

[212] The following scenario is easily imaginable:

> A suspected drug smuggler types anxiously into his [BlackBerry]. [Before arriving at the airport,] [h]e hurriedly writes an e-mail to an overseas accomplice, confirming plans for the importation of two tons of cocaine into the United States. The smuggler's highly incriminating message, if seized by law enforcement officers, could . . . place him in prison for life.

Aaron Y. Strauss, Note, *A Constitutional Crisis in the Digital Age: Why the FBI's "Carnivore" Does Not Defy the Fourth Amendment*, 20 CARDOZO ARTS & ENT. L.J. 231, 231 (2002).

[213] *Fortna*, 796 F.2d at 738.

[214] In 2001, "federal authorities seized 1,211 metric tons of marijuana," more than 111 tons of cocaine, and nearly 6,000 pounds of heroin at the border. DEA, Drug Trafficking in the United States, http://www.dea.gov/concern/drug_trafficking.html (last visited Sept. 14, 2006).

[215] Michael Freedman, *The Invisible Bankers*, FORBES, Oct. 17, 2005, at 94.

tainted profits and funds used to support terrorist networks.[216] CBP works with several other agencies to enforce the prohibition of unlicensed money-transfer businesses[217] and the carrying of currency in excess of $10,000 into or out of the country without reporting the sum to the federal government.[218] Terrorists and drug traffickers have used both of these methods "to finance their operations," capitalizing on underground banking methods "as old as the Silk Road."[219] These individuals rely heavily on an informal money transfer system that operates on the fringes of global banking: the *hawala*.[220] *Hawalas* are underground banks that allow large sums of money to be transferred from establishments such as convenience stores to destinations all over the world. [221] The

---

[216] Eric Lichtblau, *Threats and Responses: The Money Trail; Agency to Expand Units Tracing Terrorist Finances*, N.Y. TIMES, Jan. 10, 2003, at A12. Although technically a money-laundering offense under United States federal law, 18 U.S.C § 1960 (2000), the funds illegally transferred from within the United States to terrorist organizations abroad actually "start off 'clean' and become 'dirty' [at a] later [time]." Freedman, *supra* note 215.

[217] 18 U.S.C. § 1960 (making it unlawful for one to "knowingly conduct[], control[], manage[], supervise[], direct[], or own[] all or part of an unlicensed money transmitting business" and subjecting a violator to fines and/or a prison sentence of not more than five years).

[218] Lichtblau, *supra* note 216. *See* 31 U.S.C. § 5332(a) (2000) (prohibiting such transportation of more than $10,000 into or out of the United States). The USA PATRIOT Act enhanced both 18 U.S.C. § 1960 and 31 U.S.C. §5332 by sanctioning harsher punishment for money remitters and by elevating bulk cash smuggling from a currency reporting violation to a criminal offense. News Release, ICE, ICE Financial Investigative Efforts Expand to Combat Growing Money Laundering Threat (Jan. 11, 2006), http://www.ice.gov/pi/news/newsreleases/articles/060111washington.htm (last visited Sept. 14, 2006).

[219] *See* Freedman, *supra* note 215.

[220] *See id.*

[221] *Halawas*—meaning "trust" or "exchange" in Arabic—originated on the Indian subcontinent as a way for merchants to avoid being robbed as they traveled. *Id.* An individual wishing to send money abroad will visit the operator of a *hawala*, a *hawalader*, here in the U.S. The *hawalader* will accept the money and a password which will serve as the only way to identify the sender. The *hawalader* will then contact his colleague in the destination country, telling his or her partner the amount to pay the recipient and the password that will be used. The sender then tells the recipient where to go and what code to use. The money is picked up, and the two *hawaladers* settle the debt at a later time. *Id.* The identity of the sender, recipient, and the purpose for which the money will be used is rarely known by the informal bankers; at the very least this information is never recorded on paper. *Id. See also* Alan Beattie, *Informal Foreign Cash Transfers Cheaper, Says Study*, FIN. TIMES (London), Apr. 1, 2005, at 5. Nearly 20,000 *hawalas* operate in the United States. Freedman, *supra* note 215. In 2004, it is estimated that nearly thirty-five percent of the $150 billion in global transfers flowed through *hawalas*. *Id.*

Another money transfer concern for both CBP and ICE is the "black-market peso exchange," a complex money laundering system used extensively by participants in the Colombian narcotics trade. Lowell Bergman, *U.S. Companies Tangled in Web of Drug Dollars*, N.Y. TIMES, Oct. 10, 2000, at A1. The system involves

system leaves no paper trail from which one may identify the sender, the receiver, or the purpose for which the funds will be used.[222] Obtaining evidence of participation in a *hawala* is difficult and has been a major source of frustration for federal law enforcement.[223] Preventing the search and replication of electronic data would allow the concealment of the already sparse evidence that may be used to demonstrate participation in such illegal money transfers.[224] Communications indicating involvement in unlicensed remittance systems, international money laundering schemes, and plans to smuggle large amounts of currency might be viewed by CBP under existing case law, but failing to apply *Fortna* would render that authority meaningless. Without a way to duplicate hard evidence, currency smugglers and illegal money remitters will take advantage of a *Fortna* exemption for electronically stored data. Customs will be greatly hindered in its ability to shutdown the pipelines that finance terrorism and those that not only support drug cartels but cleanse their profits.[225]

Finally, the consequences of creating an exemption for digital information from search and reproduction at the border would nullify CBP's authority to enforce laws protecting minors from sexual exploitation.[226] The federal government successfully apprehends and prosecutes a large number of child pornographers and international sex tourists based on evidence CBP obtains during border searches.[227] The ability to seize pornographic images of minors in paper form is not questioned and Customs has even done so outside the border search

---

the cross border flow of large amounts of money and is a method of turning illegally earned American dollars into "clean" Colombian pesos. *Id.*

In September 2005, Abad Elfgeeh, an immigrant from Yemen, was convicted of operating an unlicensed money transfer business responsible for sending more than $21.9 million dollars overseas. *Metro Briefing New York: Brooklyn: Store Owner Guilty of Money Laundering*, N.Y. TIMES, Sept. 25, 2005, at B4. Elfgeeh directed all funds from his ice cream shop in Brooklyn. *Id.*

[222] *See* Freedman, *supra* note 215.

[223] *See id.*

[224] *See id.*

[225] *See* Lichtblau, *supra* note 216.

[226] *See* 18 U.S.C. §§ 2251-52 (2000) (prohibiting the possession, receipt, and transportation of child pornography); *see also* 18 U.S.C. § 2423 (2000) (prohibiting travel outside of the United States for the purpose of engaging in sexual acts with children under the age of eighteen).

[227] *See, e.g.*, ICE, Child-Exploitation, Operation Predator, http://www.ice.gov/pi/predator/index.htm [hereinafter Operation Predator] (last visited Aug. 30, 2006).

context.[228] But creating a sanctuary for digital information would undermine significant advances made in the fight against the sexual exploitation of minors. Immunizing from replication the files contained in laptops, disks, PDAs, and memory cards would severely debilitate CBP in the effort to stop participants in and operators of the sex tourism industry.

The advantage of allowing CBP to access computer and PDA hard drives and subsequently to reproduce information stored therein is clear. Access to all electronic devices containing personal communications and images is vital to combat terrorism, narcotics trafficking, illegal money transfers, and child pornography. In order to fully utilize its law enforcement authority, Customs must be able to reproduce evidence indicating the violation of federal law, or attempt or conspiracy to do the same. Reasonable suspicion is the most realistic standard to be applied, not to the initial search of the object in question, but only to the duplication of material contained therein.[229] Given the clandestine nature of smuggling violations and the millions of passengers processed by CBP on a daily basis, a higher standard of suspicion is impracticable.[230]

D. Existing Protections and a New CBP Policy

Existing protections imposed by case law, the federal government's finite resources, and the oath taken by CBP employees to uphold the Constitution effectively, limit the ability of Customs to search and copy electronic material. These protections, combined with the adoption of an Agency-wide non-retention policy for copied information, adequately safeguard the privacy interests of international travelers.

First, case law has imposed a variety of restrictions on the border search doctrine that serve to protect the interests of travelers entering and leaving the United States.[231] While the initial search of cargo may be conducted without suspicion, the copying of the information is subject to a higher standard.[232]

---

[228] United States v. Spence, 397 F.3d 1280, 1282-85 (10th Cir. 2005) (denying defendant's motion to suppress evidence of child pornography seized by Customs officials).

[229] *See supra* Part II.C.

[230] Customs processes over one million inbound persons each day. CBP, A Day in the Life, *supra* note 139.

[231] *See* discussion *supra* Part IV.B.

[232] United States v. Fortna, 796 F.2d 724, 738-39 (5th Cir. 1986).

Similarly, the downloading, copying, or scanning of digital information would have to be supported by an agent's reasonable suspicion. Second, CBP officers do not have general police powers.[233] Customs officials may determine if goods are being unlawfully imported because the importer has failed to pay the appropriate duties on the items or because the goods are themselves contraband.[234] Officers may enforce immigration laws and ensure that those noncitizens presenting themselves for entry are admissible and have the appropriate travel documents, entry visas, or passports.[235] However, if seized by Customs, evidence indicating the violation of state law will be suppressed in later proceedings.[236]

Third, the federal government has limited resources and although CBP possesses the authority to inspect everyone and everything crossing the border, in reality, they cannot.[237] As a practical matter, computer or PDA searches could not possibly be conducted for the 1.1 million individuals the Agency must process on a daily basis.[238] Faced with these limitations, Customs must reserve secondary inspection time for those situations in which independent circumstances indicate the need fore a more intrusive search.[239] The search and seizure of electronic evidence is most likely to occur when the traveler's unusual conduct or the presence of other incriminating items in their possession suggests the need for an agent to browse a

---

[233] People v. LePera, 611 N.Y.S.2d 394, 396 (App. Div. 1994). *See also* 19 U.S.C. § 1467 (2000). CBP is responsible for policing 317 ports of entry and over 101,900 miles of combined shoreline and land border area. CBP, A Day in the Life, *supra* note 139.

[234] 19 U.S.C. § 482 (2000); *see also LePera*, 611 N.Y.S.2d at 396-97.

[235] 8 U.S.C. § 1357 (2000).

[236] *LePera*, 611 N.Y.S.2d at 398.

[237] CBP, CBP Authority to Search, http://www.cbp.gov/xp/cgov/travel/admissability/authority_to_search.xml (last visited Sept. 15, 2006) [hereinafter CBP, Authority to Search]. Those with diplomatic status are exempt from CBP processing. *Id.*

Customs often conducts more extensive secondary inspections for individuals who appear nervous or apprehensive and who have recently traveled to or are arriving from a narcotics source country. *See, e.g.*, Kaniff v. United States, 351 F.3d 780, 782 (7th Cir. 2003) (identifying Jamaica as a narcotics source country); United States v. Gbemisola, 225 F.3d 753, 755 (D.C. Cir. 2000) (identifying Cambodia as a narcotics source country); United States v. Cardenas, 9 F.3d 1139, 1153 (5th Cir. 1993) (identifying Nigeria as a known narcotics source country); United States v. Collins, 764 F.2d 647, 649 (9th Cir. 1985) (identifying Brazil as a narcotics source country).

[238] CBP, A Day in the Life, *supra* note 139.

[239] United States v. Ickes, 393 F.3d 501, 507 (4th Cir. 2005).

computer hard drive or the contents of a BlackBerry.[240] In order to maximize limited resources, Customs utilizes the Interagency Border Inspection System (IBIS) to help determine which arriving individuals are potentially non-compliant and should be targeted for secondary inspection.[241] The efficient use of CBP time means that extensive, secondary inspections must be reserved for the appropriate occasions. An individual search of all laptops, palm pilots, and memory sticks followed by the duplication of all digitally stored information is neither realistic nor resourceful.

Additionally, the men and women who protect our borders have "sworn to uphold the Constitution."[242] As the Ninth circuit noted in *United States v. Cortez-Rocha*, these officers are not "cyborgs" set out to destroy private property and violate the privacy interest of travelers.[243] Officers are trained, experienced professionals who may be counted on to carry out their responsibilities in an "intelligent and respectful" manner.[244] Justice Breyer echoed similar sentiments in his concurring opinion in *United States v. Flores-Montano*, stating that the Agency retains records of invasive searches and the reasons such inspections are conducted.[245] This process should eliminate many concerns regarding abuse of the border authority during processing.[246] CBP officers are obligated to conduct border searches for a proper, good faith governmental

---

[240] *Id.* (noting that officers did not inspect the defendant's computer until they had discovered drug paraphernalia and photographs/video of child pornography).

[241] CBP, Authority to Search, *supra* note 237. IBIS is part of the Treasury Enforcement Communications System (TECS) and is utilized by regulatory and law enforcement personnel from the FBI, the DEA, the Bureau of Alcohol, Tobacco, and Firearms and Explosives ("ATF"), the Internal Revenue Service ("IRS"), the U.S. Coast Guard, and the U.S. Secret Service. *Id.* The system "provides the law enforcement community with . . . files of common interest . . . and keeps track of information on suspected individuals, businesses, vehicles, aircraft, and vessels." *Id.* CBP is similarly alerted when a warrant for the arrest of an inbound passenger has been issued via the Advance Passenger Information System (APIS). *Id.*

[242] United States v. Cortez-Rocha, 383 F.3d 1093, 1097 (9th Cir. 2004) (inserting additional material supporting the constitutionality of the border search), *cert. denied*, 126 S. Ct. 105 (2005), *amended by* 394 F.3d 1115 (9th Cir. 2005).

[243] *Id.*

[244] *Id.* CBP provides for such situations. If a traveler feels a search was not conducted in a professional manner, he or she may ask to speak with a Customs supervisor who is available twenty-four hours a day either at the Customs facility or by telephone. Why U.S. Customs Conducts Examinations, http://www.ncbuy.com/travel/articles.html?fid=10648 (last visited Sept. 15, 2006).

[245] United States v. Flores-Montano, 541 U.S. 149, 156 (2004) (Breyer, J., concurring).

[246] *See id.*

purpose "and . . . do not waste time on dead-end adventures."[247] Any search conducted in bad faith is invalid, and any evidence obtained from a tainted inspection will be suppressed and subsequently unavailable to federal prosecutors.[248] This good faith duty combined with limited federal resources will ensure that CBP authority to search and duplicate personal, electronically stored information is not abused.

Finally, the implementation of an Agency-wide policy similar to that mandated in *Heidy v. United States*[249] will serve as an additional element of protection for individuals who have personal information copied by Customs but who have not violated federal law. When material in paper or electronic form is searched and reproduced, Customs must be able to retain those copies until it becomes evident that the material "no longer has any evidentiary, prosecut[orial], or investigative value."[250] This enables the Agency to retain information that may lead to the successful prosecution of drug traffickers, pedophiles, or perhaps the foiling of a terrorist plot. However, once a determination is made that the evidence has no law enforcement value, the copies must be destroyed. Detailed records of a non-violation describing the nature of the search and identifying the individual from whom the information was seized must not be maintained in a federal database.[251] Further, Customs must not share photocopied or reproductions of electronic files with other law enforcement agencies unless those agencies agree to abide by CBP's policy of non-retention.[252] This will allay fears that records will be maintained and used to target individuals during future border crossings, thus inhibiting travel.[253] The adoption and application of a *Heidy* policy will allow CBP to effectively police our borders and enforce federal law while shielding travelers from an experience like that of Franz Kafka's fictional

---

[247] *Cortez-Rocha*, 383 F.3d at 1097.

[248] *See, e.g.*, Wong Sun v. United States, 371 U.S. 471, 484-88 (1963) (establishing the "fruit of the poisonous tree" doctrine).

[249] 681 F. Supp. 1445 (C.D. Cal. 1988). While the court order in *Heidy* was binding on the former U.S. Customs Service regarding the enforcement of 19 U.S.C. § 1305 (2000), which prohibits the importation of subversive material, the order is not currently binding on CBP as a new agency. Neither CBP nor the Department of Homeland Security currently has a policy addressing the maintenance of reproductions of electronic evidence.

[250] *Heidy*, 681 F. Supp. at 1447 n.6.

[251] *Id.* at 1453.

[252] *Id.*

[253] *See, e.g.*, *id.* at 1148 & n.8.

character Joseph K.[254]—knowing large amounts of personal information is in the hands of the government, but having no way to determine precisely what that information is, or for what purpose the material will be used.[255]

VI. CONCLUSION

The border search exception to the Fourth Amendment must be preserved in our increasingly digitized world.[256] Customs authority to conduct unwarranted and often suspicionless searches remains as critical to national security today as it was in the late eighteenth century when Congress passed the first customs.[257] At the border, where our protectionist interest is "at its zenith,"[258] immunity for electronic evidence from search and seizure would be disastrous.

Customs has the authority to search all persons and items crossing the border; this is undisputed.[259] This necessarily includes laptop computers, as explained in *Ickes*.[260] PDAs, memory cards, and other wireless communication devices are nearly identical to conventional laptop computers in terms of function and hard drive capabilities, differing only in size and portability. The similarities in form and function mandate the extension of the *Ickes* holdings to all portable electronic items.

The Agency's authority to copy paper evidence indicating the violation of federal, Customs-enforced law is also well settled and appropriately subjected only to a standard of

---

[254] Joseph K. is the protagonist of Franz Kafka's 1925 novel, *The Trial*. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV 1393, 1419-21 (2001). Joseph awakes one morning to find officials in his apartment. *Id.* He is arrested for reasons never revealed and subjected to judicial process by a court that has created a massive collection of data about his personal life that "'pass[es] on to the highest Courts, being referred to the lower ones again . . . . No document is ever lost, the Court never forgets anything. One day—quite unexpectedly—some Judge will take up the documents and look at them attentively . . . [a]nd the case begins all over again.'" *Id.* at 1420 (quoting FRANZ KAFKA, THE TRIAL (Willa & Edwin Muir trans., 1937)). *See also* Doe v. Se. Penn. Transp. Auth., 72 F.3d 1133, 1135-37 (3d Cir. 1995) (describing plaintiff's fear that records of his HIV status maintained in employer's database would subject him to discrimination).

[255] SOLOVE, *supra* note 159, at 67.

[256] *See supra* Part V.A.

[257] *See supra* note 41.

[258] United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

[259] *See supra* Part II.

[260] *See supra* Part III.

reasonable suspicion.[261] This authority must also be extended to modern, portable electronic devices and the large amount of information these objects may store. While the sheer volume of personal materials that can be contained in a BlackBerry or palm pilot merits special consideration, the fact remains that one may not reasonably expect privacy at the border. The medium has changed, but the logic of *Fortna* remains valid.

Existing protections coupled with a policy of non-retention adequately protect individual privacy interests. If the Agency duplicates electronically stored information during a search and later determines that the individual from whom information was seized has not and is not conspiring to violate federal law, all copies will be destroyed. The Agency would further refuse dissemination to other federal agencies unless compliance with this policy was secured.

Customs and Border Protection has a daunting role in the law enforcement sector and the enormous responsibility of policing thousands of miles of land and coastline. Failure to extend the border search doctrine and the principles of *Fortna* to all portable hand-held wireless devices and accompanying disks and memory sticks would severely handicap a federal law enforcement agency that plays a vital role in the protection of our country.

Kelly A. Gilmore[†]

---

[261] *See supra* Part IV.

[†] J.D. candidate, 2007, Brooklyn Law School.