Boston College Law Review

Volume 55
Issue 6 *Electronic Supplement*

Article 4

2-10-2014

A Step in the Wrong Direction: The Ninth Circuit Requires Reasonable Suspicion for Forensic Examinations of Electronic Storage Devices During Border Searches in *United States v. Cotterman*

Michael Creta
Boston College Law School, michael.creta@bc.edu

A STEP IN THE WRONG DIRECTION: THE NINTH CIRCUIT REQUIRES REASONABLE SUSPICION FOR FORENSIC EXAMINATIONS OF ELECTRONIC STORAGE DEVICES DURING BORDER SEARCHES IN *UNITED STATES v. COTTERMAN*

Abstract: On March 8, 2013, in *United States v. Cotterman*, the U.S. Court of Appeals for the Ninth Circuit—sitting en banc—held that U.S. border agents must have a reasonable suspicion of criminal activity before conducting a forensic search of an electronic storage device at the border. In reaching this conclusion, the court narrowed existing federal appeals court precedents, which held that manual searches of electronic storage devices do not require any suspicion. This Comment argues that a reasonable suspicion requirement is illogical, harmful to national security, and administratively impractical. Instead, strengthening existing federal regulations is a better method to protect personal privacy interests.

INTRODUCTION

Approximately sixty-two million personal vehicles crossed the U.S.-Mexican border in 2012.[1] Border agents are tasked with the duty of preventing these vehicles from transporting contraband into the United States.[2] In order to accomplish this obligation, the border search doctrine grants border agents wide discretion to conduct inspections at the border—even those that might otherwise be prohibited by the Fourth Amendment.[3] In 2013, in *Unit-*

---

[1] *Border Crossing/Entry Data: Query Detailed Statistics*, RESEARCH & INNOVATIVE TECH. ADMIN. BUREAU OF TRANSP. STAT., http://transborder.bts.gov/programs/international/transborder/TBDR_BC/TBDR_BCQ.html (last visited Jan. 19, 2014) (select "Southern Border Ports" for "Port Location"; select "2012" for "Year"; select "Annual Summary" for "Month"; select "Aggregate All Southern Border Ports" for "Port Name"; select "All Measures Detail" for "Measure"; click "Submit"), *archived at* http://perma.cc/KH8M-7MLC?type=pdf.

[2] United States v. Cotterman (*Cotterman III*), 709 F.3d 952, 971 (9th Cir. 2013) (en banc) (Callahan, J., concurring in part and concurring in the judgment), *cert. denied*, 82 U.S.L.W. 3095 (U.S. Jan. 13, 2014) (No. 13-186).

[3] *Id.*; Ickes v. United States, 393 F.3d 501, 507 (4th Cir. 2005); *see* United States v. Martinez-Fuerte, 428 U.S. 543, 563–64 (1976) (indicating that border agents have "wide discretion" when determining which vehicles to search at the border).

ed States v. Cotterman (Cotterman III), the U.S. Court of Appeals for the Ninth Circuit limited this discretion by requiring agents to possess a reasonable suspicion of criminal activity before conducting a forensic examination of an electronic storage device during a border search.[4] The court reasoned that electronic storage devices are unlike traditional storage devices, such as suitcases or car trunks, and therefore warrant heightened Fourth Amendment protection.[5]

Part I of this Comment discusses the Fourth Amendment, the border search doctrine, and the recent federal directives regarding searches of electronically stored information.[6] Then, it addresses the *Cotterman III* court's holding that the district court erred in granting Cotterman's motion to suppress evidence gathered from his laptop.[7] Part II examines the alternative approaches to border searches of electronic storage devices utilized by other federal appeals courts and, further, how *Cotterman III* narrowed existing circuit precedent by requiring reasonable suspicion for forensic examinations.[8] Lastly, Part III argues that the Ninth Circuit's decision was both illogical and administratively impractical, and served to protect personal privacy rights at the expense of national security.[9] Part III concludes that executive directives governing the scope of forensic examinations of electronic storage devices are a practical alternative that can strike a more appropriate balance between personal privacy and national security.[10]

I. The Fourth Amendment and its Implications During a Crossing of the U.S. Border

A. *The Border Search Doctrine*

The Fourth Amendment of the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[11] For a search to be reasonable, state actors must obtain a warrant based on probable cause.[12]

---

[4] *See Cotterman III*, 709 F.3d at 968. The court described the forensic examinations of electronic storage devices as a "powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on websites." *Id.* at 957.

[5] *Id.* at 964–66, 968.

[6] *See infra* notes 11–25 and accompanying text.

[7] *See infra* notes 26–41 and accompanying text.

[8] *See infra* notes 42–72 and accompanying text.

[9] *See infra* notes 73–97 and accompanying text.

[10] *See infra* notes 98–113 and accompanying text.

[11] U.S. Const. amend. IV.

[12] *See* Chambers v. Maroney, 399 U.S. 42, 51 (1975) (stating that probable cause is a "minimum requirement for a reasonable search permitted by the Constitution"); Camara v. Mun. Court, 387 U.S. 523, 534 (1967) (noting that probable cause is the standard used to determine if a search is constitutionally reasonable).

Probable cause is defined as "[a] reasonable ground to suspect that a person has committed or is committing a crime or that a place contains specific items connected with a crime."[13]

For border searches, however, the U.S. Supreme Court has indicated that no suspicion is required for a search to be constitutionally reasonable under the Fourth Amendment.[14] A border search is a search conducted at a U.S. border to detect illegal aliens or contraband.[15] Therefore, it follows that border searches are an exception to the Fourth Amendment's requirement of a warrant based on probable cause.[16]

Despite this exception, some border searches may require a reasonable suspicion of criminal activity.[17] The Court has defined a reasonable suspicion as "a particularized and objective basis for suspecting the particular person" of transporting contraband.[18] In 2004, in *United States v. Flores-Montano*, the U.S. Supreme Court provided three categories of border searches that may require reasonable suspicion: "(1) highly intrusive searches of the person; (2) destructive searches of property; and (3) searches conducted in a particularly offensive manner."[19] Today, for border

---

[13] BLACK'S LAW DICTIONARY 1321 (9th ed. 2009).

[14] United States v. Ramsey, 431 U.S. 606, 616 (1977) (noting that "searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border").

[15] BLACK'S LAW DICTIONARY, *supra* note 13, at 1468.

[16] *See* Witt v. United States, 287 F.2d 389, 391 (9th Cir. 1961) (holding that merely crossing the border is a sufficient reason to search a person); *see also* Marsh v. United States, 344 F.2d 317, 324 (5th Cir. 1965) ("A true border search . . . is not regarded as unreasonable even though made without probable cause."); Murgia v. United States, 285 F.2d 14, 17 (9th Cir. 1960) ("The right of border search does not depend on probable cause."). This border search exception was first established by a customs statute passed by Congress in 1789. *See* Act of July 31, 1789, ch. 5, §§ 23–24, 1 Stat. 29, 43; *see also Ramsey*, 431 U.S. at 616 (stating that the border search exception existed before the Fourth Amendment was proposed). *See generally* Jules D. Barnett, *A Report on Search and Seizure at the Border (Customs Problems)*, 1 AM. CRIM. L. Q., Aug. 1963, at 36 (discussing the Act of July 31, 1789 and subsequent border search legislation). In 1977, in *United States v. Ramsey*, the U.S. Supreme Court officially recognized the exception. 431 U.S. at 619 (internal quotation marks omitted) (reaffirming the "longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless reasonable"). Today, customs agents continue to enjoy the ability to conduct searches at the border without probable cause or a warrant. *See* 19 U.S.C. § 482(a) (2006) (allowing agents to search "any vehicle, beast, or person" for merchandise which "may have been introduced into the United States in any manner contrary to law").

[17] *See* United States v. Flores-Montano, 541 U.S. 149, 152, 155–56 & n.2 (2004).

[18] United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985); *see also* United States v. Cortez, 449 U.S. 411, 417–18 (1981).

[19] *Flores-Montano*, 541 U.S. at 152–56 & n.2; *see Cotterman III* 709 F.3d at 973 (Callahan, J., concurring in part and concurring in the judgment) (internal quotation marks omitted) (quoting *Flores-Montano*, 541 U.S. at 152–56 & n.2). Under this framework, the Court held that the removal, disassembly, and reassembly of a vehicle's gas tank was not so destructive as to require U.S. border agents to have a reasonable suspicion of criminal activity. *Flores-Montano*, 541 U.S. at 155–56. A search of a traveler's alimentary canal, however, is one example of a "highly intrusive search of a person." *See Montoya de Hernandez*, 473 U.S. at 541. The Court has never held a search to be "particularly offensive." *Cotterman III*, 709 F.3d at 982 (Smith, J., dissenting).

searches of property, it appears that lower courts should determine if either of the latter two above categories is applicable.[20]

In August 2009, the Department of Homeland Security (DHS) issued new directives to U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) to protect personal privacy interests by restricting how information gathered from confiscated electronic devices can be used.[21] Described as "guidelines," the directives create substantial limitations on the retention, sharing, and destruction of confiscated data.[22] For example, the CBP directive requires all searches of electronic devices to be completed as "expeditiously as possible."[23] Furthermore, according to this directive, all detentions of devices should not last longer than five days, and managers must approve any detention that exceeds five days.[24] Additionally, if a CBP agent determines that there is no probable cause for retaining copied information, the information must be destroyed within seven days.[25]

B. *Venturing Across the Border with 453 Images of Child Pornography*

On April 6, 2007, Howard Cotterman and his wife attempted to enter the United States from Mexico at the Lukeville, Arizona Port of Entry ("POE").[26] During the U.S. border agents' initial inspection, the Treasury Enforcement Communication System ("TECS") returned a hit indicating that Cotterman was a sex offender.[27] Because of this TECS hit, border

---

[20] *See Flores-Montano*, 541 U.S. at 155–56 & n.2 (indicating that some searches of property may be so destructive or offensive as to require reasonable suspicion).

[21] *See* U.S. CUSTOMS & BORDER PROT., DIRECTIVE 3340-049, BORDER SEARCHES OF ELECTRONIC DEVICES CONTAINING INFORMATION 1 (2009); U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, DIRECTIVE 7-6.1, BORDER SEARCHES OF ELECTRONIC DEVICES 1 (2009).

[22] *See* U.S. CUSTOMS & BORDER PROT., *supra* note 21, at 4; U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, *supra* note 21, at 7–8; Rachel Flipse, Comment, *An Unbalanced Standard: Search and Seizure of Electronic Data Under the Border Search Doctrine*, 12 U. PA. J. CONST. L. 851, 858 (2010) (discussing the directives' limitations regarding confiscated data).

[23] U.S. CUSTOMS & BORDER PROT., *supra* note 21, at 4.

[24] *Id.*

[25] *Id.* In any event, the ICE directive mandates that all information gathered from electronic devices be destroyed within twenty-one days of the initial search. U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, *supra* note 21, at 8.

[26] United States v. Cotterman (*Cotterman II*), 637 F.3d 1068, 1070–71 (9th Cir. 2011), *rev'd en banc*, 709 F.3d 952 (9th Cir. 2013).

[27] *Cotterman III*, 709 F.3d at 957. TECS is an "information sharing platform" that acts as a primary tool for border agents to determine if individuals should be admitted into the country. JACQUELINE RUSSELL-TAYLOR, DEP'T OF HOMELAND SEC., DHS/CBP/PIA-009(A), TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING (TECS) NATIONAL SAR INITIATIVE 2 (2011). The TECS hit indicated that Cotterman had a 1992 conviction for two counts of use of a minor in sexual conduct, two counts of lewd and lascivious conduct upon a child, and three counts of child molestation. *Cotterman III*, 709 F.3d at 957.

agents conducted a secondary inspection and recovered two laptop computers and three digital cameras.[28] After discovering inaccessible password-protected files on one laptop, agents from the ICE office detained the Cottermans' devices for a full forensic examination.[29]

Two days later, an ICE agent discovered seventy-five images of child pornography on one of the confiscated laptops.[30] When a border agent contacted Cotterman, he fled to Mexico, and then continued on to Sydney, Australia.[31] On June 27, 2007, Cotterman was indicted in the U.S. District Court for the District of Arizona for production of child pornography, transportation and shipping of child pornography, importation of obscene material, and unlawful flight to avoid prosecution.[32] After being charged, Australian law enforcement arrested Cotterman and extradited him to Arizona.[33]

Upon return to Arizona, Cotterman moved to suppress all evidence that was recovered from his laptop.[34] He argued that reasonable suspicion of criminal activity was needed before the border agents could search his laptop, and that the agents lacked such suspicion.[35] Pursuant to a Report and Recommendation from a Magistrate Judge, the district court granted the motion to suppress in full because the border agents had conducted an extended border search in the absence of reasonable suspicion.[36]

---

[28] *Cotterman III*, 709 F.3d at 957.

[29] *Id.* at 957–58; *see supra* note 4 (describing a forensic examination).

[30] *Cotterman III*, 709 F.3d at 958.

[31] *Id.* at 959. Two days after Cotterman fled, an ICE agent accessed Cotterman's password-protected files and uncovered an additional 378 images of child pornography. *Cotterman II*, 637 F.3d at 1073.

[32] *Cotterman II*, 637 F.3d at 1073.

[33] *Id.*

[34] Defendant's Motion to Suppress Evidence & Request for Evidentiary Hearing at 1, United States v. Cotterman (*Cotterman I*), No. CR 07-1207-TUC-RCC (D. Ariz. Feb. 24, 2009), 2009 WL 465028, ECF No. 17.

[35] *Id.* at 6.

[36] United States v. Cotterman (*Cotterman I*), No. CR 07-01207-TUC-RCC, 2009 WL 465028, at *9–10 (D. Ariz. Feb. 24, 2009), *rev'd en banc*, 709 F.3d 952 (9th Cir. 2009). In his Recommendation, Magistrate Judge Charles Pyle held that the forensic examination was an extended border search because it was conducted two days after the initial search at a location approximately 170 miles away from the Lukeville POE. Report and Recommendation at 13, United States v. Cotterman, No. CR 4:07-01207-RCC-CRP (D. Ariz. Sept. 12, 2008), ECF No. 52. Extended border searches are an additional category of searches that require reasonable suspicion. United States v. Alfonso, 759 F.2d 728, 734 (9th Cir. 1985); United States v. Garcia, 672 F.2d 1349, 1366–67 (11th Cir. 1982). An extended border search involves a warrantless search conducted away from the border or its functional equivalent after the "first point in time when the entity might have been stopped within the country." United States v. Cardenas, 9 F.3d 1139, 1148 (5th Cir. 1993). Extended border searches require a reasonable suspicion of criminal activity because they involve a greater intrusion on privacy interests than searches conducted at the border. *See* United States v. Niver, 689 F.2d 520, 526 (5th Cir. 1982). A substantial number of district court cases, including *Cotterman I*, have treated forensic examinations of laptops away from the border as extended border searches. *See, e.g.*, United States v. Hanson, CR 09-00946 JSW, 2010 WL 2231796, at *4

On appeal, the U.S. Court of Appeals for the Ninth Circuit—sitting en banc—held that the district court erred in granting Cotterman's motion to suppress.[37] Previously, a divided panel of the court held in *Cotterman II* that the search was not an extended border search requiring reasonable suspicion.[38] When sitting en banc, the *Cotterman III* court also held that the search did not qualify as an extended border search.[39] Despite this holding, the en banc court also held that reasonable suspicion was still necessary to conduct the search—due primarily to the nature of the property being searched.[40] Unlike the district court, however, the court ruled that there was a reasonable suspicion of criminal activity and thus the evidence was admissible.[41]

II. Searches of Electronic Storage Devices: A Suspicionless or Reasonable Suspicion Standard?

While the border search doctrine has existed for hundreds of years, electronic storage devices are a more recent invention.[42] Today, courts must determine to what extent the longstanding border search doctrine can be applied to new technologies.[43] Section A of this Part discusses the landscape of federal court cases analyzing searches of electronic storage devices prior to the U.S. Court of Appeals for the Ninth Circuit's 2009 decision in *United States v. Cotterman (Cotterman III)*.[44] Section B of this Part discusses the *Cotterman III* court's narrowing of these precedents.[45]

(N.D. Cal. June 2, 2010); United States v. Stewart, 715 F. Supp. 2d 750, 755 (E.D. Mich. 2010); *Cotterman I*, 2009 WL 465028, at *9. This case law is beyond the scope of this brief Comment because the *Cotterman III* court held that the forensic examination of Cotterman's laptop was not an extended border search. 709 F.3d at 962.

[37] *Cotterman III*, 709 F.3d at 970.

[38] *Cotterman II*, 637 F.3d at 1079, 1083–84 (holding that the Fourth Amendment does not require reasonable suspicion for all secondary inspections of property seized at the border).

[39] *Cotterman III*, 709 F.3d at 962 ("A border search is not transformed into an extended border search simply because the device is transported and examined beyond the border.").

[40] *See id.* at 964–66, 968 (holding that the unique qualities of laptops require reasonable suspicion for forensic examinations).

[41] *Id.* at 970.

[42] *See* United States v. Ramsey, 431 U.S. 606, 616 (1977) (indicating that the border search exception has existed in some form since 1789).

[43] *See* Yule Kim & Anna C. Henning, Cong. Research Serv., RL34404, Border Searches of Laptop Computers and Other Electronic Storage Devices 3, 7 (2008) (stating that federal courts must decide "whether the border search exception applies to electronic storage devices, and if it does, what degree of suspicion is needed to justify a warrantless search").

[44] *See infra* notes 46–59 and accompanying text.

[45] *See infra* notes 60–72 and accompanying text.

A. *A Universal Circuit Precedent: Suspicionless Searches of Electronic Storage Devices*

Prior to *Cotterman III*, numerous circuit courts—the Third, Fourth, and Ninth circuits—unanimously held that searches of electronic storage devices at the border did not require reasonable suspicion of criminal activity.[46] According to this precedent, the *Cotterman II* panel held that electronic storage devices could be searched without reasonable suspicion.[47]

Courts upholding suspicionless border searches of electronic storage devices reason that reasonable suspicion is not required if none of the *Flores-Montano* exceptions apply.[48] In 2008, in *United States v. Arnold*, the U.S. Court of Appeals for the Ninth Circuit held that reasonable suspicion is not required to search an electronic storage device at the border.[49] The court rejected the defendant's arguments primarily through an application of the *Flores-Montano* exceptions.[50] The court reasoned that the search of the laptop was not "destructive," because the defendant never argued that his laptop was damaged.[51] Further, the court held that simply turning on a laptop and looking at files would not qualify as being "particularly offensive."[52]

At least one court has reasoned that national security concerns, logistical difficulties, and U.S. Supreme Court precedent justify suspicionless border searches of electronic storage devices.[53] In 2005, in *United States v. Ickes*, the U.S. Court of Appeals for the Fourth Circuit upheld suspicionless

---

[46] *See* United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008); United States v. Linarez-Delgado, 259 F. App'x. 506, 508 (3d Cir. 2007); United States v. Ickes, 393 F.3d 501, 507–08 (4th Cir. 2005).

[47] *Cotterman II*, 637 F.3d 1068, 1083–84 (9th Cir. 2011), *rev'd en banc*, 709 F.3d 952 (9th Cir. 2013).

[48] *See Arnold*, 533 F.3d at 1008–10; United States v. Hernandez, 424 F.3d 1056, 1059 (9th Cir. 2005); *supra* note 19 and accompanying text (discussing the exceptions that the U.S. Supreme Court established in its 2004 *United States v. Flores-Montano* decision); *see also* United States v. Flores-Montano, 541 U.S. 149, 152, 155–56 & n.2 (2004).

[49] *Arnold*, 533 F.3d at 1008. In *Arnold*, the defendant flew from the Philippines to the Los Angeles International Airport with a laptop that contained a collection of child pornography. *Id.* at 1005. The *Arnold* decision was not the first time that the Ninth Circuit refused to require reasonable suspicion for laptop searches. *See* United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006) (declining to consider if a search of a laptop requires reasonable suspicion).

[50] *Arnold*, 533 F.3d at 1008–09 (citing *Flores-Montano*, 541 U.S. at 155–56 & n.2); *see supra* note 19 and accompanying text (discussing the *Flores-Montano* exceptions). In *Arnold*, the defendant argued that reasonable suspicion was required because "laptop computers are fundamentally different from traditional closed containers," and because the First Amendment requires a reasonable suspicion requirement for border searches of expressive materials. *Arnold*, 533 F.3d at 1006.

[51] *Id.* at 1009.

[52] *Id.*

[53] *See Ickes*, 393 F.3d at 506–07 (citing New York v. P.J. Video, 475 U.S. 868, 874 (1986); *Ramsey*, 431 U.S. at 620).

border searches of electronic storage devices.[54] In *Ickes*, the court rejected the defendant's argument that the border search doctrine did not apply to "expressive" items that are protected by the First Amendment.[55]

Guided by the *Ickes* and *Arnold* rulings, in 2011, in *Cotterman II*, a panel of the U.S. Court of Appeals for the Ninth Circuit held that a reasonable suspicion of criminal activity was not required for U.S. border agents to search Cotterman's laptop.[56] The panel applied the *Flores-Montano* exceptions, and focused on whether the forensic examination of the laptop away from the border was "particularly offensive."[57] The court held that such searches are not necessarily offensive, as some searches of electronic storage devices require "complex equipment and technical personnel" that cannot be located at the POE.[58] Further, a search does not become unreasonable solely because it continues for an extended period of time.[59]

---

[54] *See Ickes*, 393 F.3d at 507–08. There, the defendant attempted to cross the U.S.-Canadian border in a van containing a collection of contraband, including a computer with approximately seventy-five disks of child pornography. *Id.* at 502–03.

[55] *Id.* at 506. The defendant in *Ickes* made this argument in an effort to persuade the court that his computer and disks were "expressive" and therefore outside of the scope of the border search doctrine. *Id.* The court rejected this argument for three reasons. *Id.* at 506–07. First, the court indicated that a First Amendment exception to the border search doctrine would impair national security by creating a "sanctuary at the border for all expressive material," which could possibly include terrorist communications. *Id.* Second, the court noted that it would be difficult for border agents to determine exactly what type of expressive items are covered by the First Amendment exception. *Id.* Third, the court noted that in its 1986 decision *New York v. P.J. Video*, the U.S. Supreme Court was unwilling to create a First Amendment exception for expressive items in the context of warrant applications. *Id.* at 507 (citing *P.J. Video*, 475 U.S. at 874 (refusing to require a heightened standard of probable cause for warrant applications when expressive items are involved); *Ramsey*, 431 U.S. at 620 (stating that it was unnecessary to consider the First Amendment in the border search context)). The *Arnold* court also adhered to the *Ickes'* court's reasoning when it refused to create a First Amendment exception to the border search doctrine. *Arnold*, 533 F.3d at 1010 (citing *Ickes*, 393 F.3d at 506–08).

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

[57] *Id.* at 1080. According to Cotterman, the U.S. border agents could have discovered the child pornography at the POE if they had conducted a forensic search there or had accepted his offer to help them access password-protected files. *Id.* Therefore, Cotterman argued that the forensic examination of the laptops away from the border was "particularly offensive" because it could have been conducted at the border and also involved an extensive amount of time. *Id.* The court quickly determined that the other two *Flores-Montano* exceptions—highly intrusive searches of the person and destructive searches of property—did not apply. *Id.*

[58] *Id.* at 1081–82.

[59] *Id.* at 1082 ([W]e have . . . consistently rejected hard-and-fast time limits . . . . [C]ommon sense and ordinary human experience must govern over rigid criteria." (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 542–44 (1985)) (internal quotation marks omitted)).

B. *The Ninth Circuit Establishes a New Requirement of Reasonable Suspicion for Forensic Examinations of Electronic Storage Devices*

In *Cotterman III*, the U.S. Court of Appeals for the Ninth Circuit—sitting en banc—narrowed existing federal circuit precedent by reversing the decision of the *Cotterman II* panel and establishing a reasonable suspicion requirement for forensic examinations of electronic storage devices.[60] The court, emphasizing the need to protect "substantial personal privacy interests," held that electronic storage devices should be treated differently than traditional storage devices because they have unique characteristics.[61] The court reasoned that these unique characteristics make any search of an electronic storage device a "particularly offensive" search, which requires reasonable suspicion.[62]

The court highlighted three characteristics of electronic storage devices that render searches of such materials "particularly offensive."[63] First, the court stressed that these devices have immense storage capacities and contain large amounts of private information.[64] Accordingly, electronic storage

---

[60] *See Cotterman III*, 709 F.3d 952, 968 (9th Cir. 2013) (en banc), *cert. denied*, 82 U.S.L.W. 3095 (U.S. Jan. 13, 2014) (No. 13-186). Because the court held that a manual search of electronic files would not require reasonable suspicion, *Cotterman III* does not directly conflict with either *Ickes* or *Arnold*, both of which also held that manual searches of laptops did not require reasonable suspicion. *See id.* at 967; *Arnold*, 533 F.3d at 1008; *Ickes*, 393 F.3d at 507–08. A manual search requires that border agents access individual files by hand, where a forensic search involves complex technology that copies and searches an electronic storage device's hard drive. *See Cotterman III*, 709 F.3d at 958 (forensic search); *Arnold*, 533 F.3d at 1005 (manual search). While the *Cotterman III* court limited its holding to forensic examinations, its analysis focused on how electronic storage devices are different than traditional storage devices, rather than on how forensic searches are more intrusive than manual searches. *See Cotterman III*, 709 F.3d at 964–66.

[61] *See Cotterman III*, 709 F.3d at 964–66. The *Cotterman III* court treated laptops as a unique category of property deserving special protection under the Fourth Amendment; while other courts have treated all forms of property equally. *Compare Cotterman III*, 709 F.3d at 966 (stating that the constitutional inquiry of reasonableness "must account for differences in property"), *with* United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008) (stating that "[t]he format of a record or document should not be dispositive to a Fourth Amendment inquiry"), *Arnold*, 533 F.3d at 1009 (stating that the U.S. Supreme Court has "refused to draw distinctions between [different] containers of information"), *and Ickes*, 393 F.3d at 507 (holding that "expressive material" would not be treated differently). While courts, until *Cotterman III*, have avoided treating laptops as a special category of property, some in the academic community have been more willing to afford special protection to electronic storage devices. *See* Christine A. Coletta, Note, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 B.C. L. REV. 971, 999 (2007) (arguing that a "laptop is substantively different from a wallet").

[62] *See Cotterman III*, 709 F.3d at 964–66, 968. It is unclear which of the three *Flores-Montano* exceptions the majority opinion relies upon in *Cotterman III*. *See id.* at 973 (Callahan, J., concurring in part and concurring in the judgment). But, because a laptop is not a person and there were no allegations of destruction, it appears that the majority holds that a forensic examination of an electronic storage device qualifies as "particularly offensive." *See id.*

[63] *Id.* at 964–66 (majority opinion); *see infra* notes 64–72 and accompanying text (discussing the three characteristics that make searches of electronic storage devices "particularly offensive").

[64] *Cotterman III*, 709 F.3d at 964.

devices, in the view of the court, are unlike traditional storage devices due to their ability to contain "warehouses of information."[65]

Second, the court explained that the nature of electronically stored content is different from that of traditional storage devices.[66] Electronic storage devices contain "the most intimate details of our lives."[67] The court stated that electronic storage devices are "simultaneously offices and personal diaries."[68]

Third, the court observed that it is often difficult to effectively remove data from electronic storage devices.[69] Electronic storage devices may "retain sensitive and confidential information far beyond the perceived point of erasure."[70] For the court, this retention of "deleted" data is significant because it makes it difficult for an international traveler to withhold any digital information from inspection.[71] Besides the ability to retain "deleted" data, the court also noted that, for most travelers, removing certain files prior to crossing the border is not a practical method of maintaining privacy.[72]

III. Reasonable Suspicion: A Clumsy Solution to a Complicated Problem

U.S. border agents should be able to conduct forensic examinations of electronic storage devices with minimal suspicion.[73] A suspicionless search standard avoids the creation of arbitrary distinctions between different types of property.[74] Moreover, suspicionless searching is a clear standard that al-

---

[65] *Id.* The court points out that a 400 gigabyte laptop could hold over 200 million pages of paper. *Id.* (citing Orin S. Kerr, *Searches and Seizures in the Digital World*, 119 Harv. L. Rev 531, 542 (2005) (explaining that an eighty gigabyte hard drive can hold forty million pages of paper)).

[66] *Id*.

[67] *Id.* At least one academic author also argues that electronic storage devices should be excluded from traditional Fourth Amendment doctrines because they are "reasonably likely to contain intimate personal information." Joshua A. Engel, *Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices*, 41 U. Mem. L. Rev. 233, 297 (2010).

[68] *Cotterman III*, 709 F.3d at 964.

[69] *Id.* at 965.

[70] *Id.*; *see also* Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Laws Based on Images Located in Temporary Internet Files*, 19 Berkeley Tech. L.J. 1227, 1228 (2004) (stating that "computer-based evidence is not easily destroyed without specialized knowledge").

[71] *Cotterman III*, 709 F.3d at 965.

[72] *Id.*

[73] *See Cotterman II*, 637 F.3d 1068, 1083–84 (9th Cir. 2011), *rev'd en banc*, 709 F.3d 952 (9th Cir. 2013); United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 507–08 (4th Cir. 2005).

[74] *See* Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. Rich. L. Rev. 1091, 1093 (2009) ("[P]rivacy protections travelers enjoy should not depend on whether they store their data in digital format or on paper.").

lows U.S. border agents to detect criminal activity.[75] Instead of changing the legal standard for searches, the existing CBP and ICE directives should be strengthened to limit the sharing and retention of digitally acquired information.[76] Focusing on how information is used, as opposed to when it can be collected, is an administratively practical standard that avoids tampering with constitutional doctrine and also strikes an appropriate balance between border protection goals and personal privacy interests.[77]

To determine if reasonable suspicion is required, courts should focus on the manner in which a border search is conducted, rather than on the inherent qualities of the property being searched.[78] Because electronic storage devices often serve the same functional purposes as traditional storage devices, treating the two categories of property equally is logical.[79] Suitcases, luggage, and any other traditional storage containers are always subjected to suspicionless border searches even if they contain large amounts of personal information.[80] Merely converting the personal information contained in a suitcase into an electronic form should not be enough to bestow heightened constitutional protection.[81] Indeed, the U.S. Supreme Court has long held

---

[75] *See Cotterman III*, 709 F.3d 952, 979 (9th Cir. 2013) (en banc) (Callahan, J., concurring in part and concurring in the judgment), *cert. denied*, 82 U.S.L.W. 3095 (U.S. Jan. 13, 2014) (No. 13-186) (suggesting that a reasonable suspicion requirement will make it more difficult for U.S. border agents to conduct meaningful searches); *id.* at 982 (Smith, J., dissenting) (stating that reasonable suspicion is "administratively impractical"); Kelly A. Gilmore, Note, *Preserving the Border Search Doctrine in a Digital World*, 72 BROOK. L. REV. 759, 781 (2007) (arguing that U.S. border agents must be able to conduct suspicionless searches to protect the country from "terrorism, narcotics trafficking, illegal money transfers, and child pornographers").

[76] *See* Flipse, *supra* note 22, at 858–59 (arguing that existing federal regulations have made progress but still do not provide travelers with enough protection); Gilmore, *supra* note 75, at 781 (arguing for a "new CBP policy providing for the destruction of copied materials"); *supra* notes 21–25 and accompanying text (discussing the CBP and ICE directives).

[77] *See* Sales, *supra* note 74, at 1124; Sunil Bector, Note, *"Your Laptop, Please:" The Search and Seizure of Electronic Devices at the United States Border,* 24 BERKELEY TECH. L.J. 695, 716–17 (2009).

[78] *See Cotterman III*, 709 F.3d at 988 (Smith, J., dissenting) (indicating that the U.S. Supreme Court in its 2004 *United States v. Flores-Montano* decision did not distinguish between types of property); *see also* United States v. Flores-Montano, 541 U.S. 149, 152, 155–56 & n.2 (2004).

[79] *See* Erick Lucadamo, Note, *Reading Your Mind at the Border: Searching Memorialized Thoughts and Memories on Your Laptop and* United States v. Arnold, 54 VILL. L. REV. 541, 570 (2009) (arguing that laptops are only digital versions of preexisting modes of storage).

[80] *See* United States v. Ross, 456 U.S. 798, 823 (1982) (stating that an international traveler's luggage may be searched "no matter how great the traveler's desire to conceal the contents may be"); Lucadamo, *supra* note 79, at 572–73 (explaining that U.S. border agents have always possessed the authority to conduct suspicionless searches of "large sailing vessels" that may contains thousands of items).

[81] *See Cotterman III*, 709 F.3d at 987 (Smith, J., dissenting) (stating that affording digitalized information added constitutional protection is both artificial and arbitrary); Sales, *supra* note 74, at 1115 (arguing that it is illogical to treat identical information differently based on where the information is stored).

that, for purposes of the Fourth Amendment, the characteristics of the property being searched are irrelevant.[82]

Furthermore, unlike the court's approach in *Cotterman III*, treating all forms of property the same does not create line-drawing problems.[83] For example, if all property is treated equally, courts would not need to determine exactly how many gigabytes a hard drive must have before it qualifies for reasonable suspicion protection.[84] Using storage capacity, as well as any other characteristic, as a criterion for granting reasonable suspicion protection is simply not feasible.[85]

Additionally, a suspicionless border search standard helps U.S. border agents to maintain national security and thwart criminal activities.[86] Affording electronic storage devices reasonable suspicion protection would only make it more difficult to combat issues such as child pornography and terrorism.[87] The government's interest in preventing harmful contraband from entering the country is at its peak at the border.[88] Without the ability to conduct suspicionless forensic examinations, it will be more difficult for U.S. border agents to prevent images of child pornography and terrorist plans from entering the country.[89] For example, a member of Al-Qaeda could store encrypted files of plans to bomb a federal building on his laptop before crossing the border, knowing that U.S. border agents cannot search any

---

[82] *See* United States v. Ramsey, 431 U.S. 606, 620 (1977) ("It is clear that there is nothing in the rationale behind the border-search exception which suggests that the mode of entry will be critical."). Prior to the U.S. Court of Appeals for the Ninth Circuit's 2013 ruling in *Cotterman III*, the court had also held that the characteristics of searched property did not affect a Fourth Amendment analysis. *See* United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008) (stating that "neither the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth Amendment context"); *see also supra* note 61 and accompanying text (discussing other federal appeals courts that had declined to treat laptops differently than other property). The academic community sometimes refers to the concept of treating property equally as "technology neutrality." *See* Sales, *supra* note 74, at 1114–15; Benjamin Rankin, Note, *Restoring Privacy at the Border: Extending the Reasonable Suspicion Standard for Laptop Border Searches*, 43 COLUM. HUM. RTS. L. REV. 301, 345 (2011).

[83] *See* Sales, *supra* note 74, at 1113; *see also Cotterman III*, 709 F.3d at 977–78 (Callahan, J., concurring in part and concurring in the judgment) (arguing that distinguishing between electronic storage devices and traditional storage devices is arbitrary).

[84] *See* Sales, *supra* note 74, at 1113 (explaining that it would be impossible for a court to determine size requirements for a hard drive to qualify for reasonable suspicion protection).

[85] *See id.* (advocating for a uniform rule for both traditional and electronic storage devices).

[86] *See* Gilmore, *supra* note 75, at 781; Lucadamo, *supra* note 79, at 574.

[87] *See* Gilmore, *supra* note 75, at 781; Lucadamo, *supra* note 79, at 574.

[88] *Flores-Montano*, 541 U.S. at 152 ("The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.").

[89] *See* U.S. CUSTOMS & BORDER PROT., *supra* note 21, at 1; Lucadamo, *supra* note 79, at 574; *see also Ickes*, 393 F.3d at 507 (observing that prohibiting suspicionless searches of expressive material would create a "sanctuary at the border . . . for terrorist plans").

encrypted files without reasonable suspicion.[90] The *Cotterman III* court created a legal loophole for technologically-sophisticated criminals.[91]

Finally, unlike searches requiring reasonable suspicion, suspicionless border searches provide a practical legal standard.[92] Every year, U.S. border agents conduct millions of border searches.[93] These agents do not have the time or the resources to determine on a case-by-case basis if there is a reasonable suspicion of criminal activity.[94] Even if a particular POE is not well traveled, U.S. border agents are not trained to make complex legal judgments.[95] Agents will be hesitant to conduct forensic examinations that could result in civil liability if a court later determines that reasonable suspicion was absent at the time of the search.[96] Suspicionless searches avoid these administrative problems because U.S. border agents are not asked to make legal conclusions.[97]

While electronic storage devices do not deserve heightened constitutional protection for all of the above reasons, the information gathered from these devices should be closely governed by agency regulations.[98] U.S. border agents have the ability to copy data from confiscated hard drives to government-owned devices.[99] This data can then be shared with a variety of government agencies or even retained for an indefinite period of time with-

---

[90] *See Cotterman III*, 709 F.3d at 985 (Smith, J., dissenting). There is abundant evidence that terrorists use electronic storage devices to plan and carry out attacks. Gilmore, *supra* note 75, at 777–78 (discussing several notable examples of terrorists using electronic storage devices).

[91] *See Cotterman III*, 709 F.3d at 985 (Smith, J., dissenting); Gilmore *supra* note 75, at 786.

[92] *See Cotterman III*, 709 F.3d at 979 (Callahan, J., concurring in part and concurring in the judgment); *id.* at 982 (Smith, J., dissenting).

[93] DEP'T OF HOMELAND SEC. PRIVACY OFFICE, ANNUAL REPORT TO CONGRESS 54 (2009).

[94] *See* United States v. Martinez-Fuerte, 428 U.S. 543, 557 (1976) (explaining that reasonable suspicion for every vehicle search at the U.S.-Mexican border would be impossible due to the large volume of travelers).

[95] *See Cotterman III*, 709 F.3d at 984 (Smith, J., dissenting) (reasoning that requiring complex legal judgments "strips agents of their necessary discretion and deprives them of an administrable rule"); *Arnold*, 533 F.3d at 1010 (citing *Ickes*, 393 F.3d at 506) (forcing border agents to decide "on their feet" if property is "expressive" would be an unworkable legal standard).

[96] *See Cotterman* III, 709 F.3d at 979 (Callahan, J., concurring in part and concurring in the judgment) (observing that U.S. border agents may avoid conducting forensic examinations of electronic storage devices rather than risk making an incorrect legal judgment).

[97] *See id.* at 984 (Smith, J., dissenting).

[98] *See* Sales, *supra* note 74, at 1133–34 (arguing that congressional or executive reform is preferable to the Fourth Amendment); Bector, *supra* note 77, at 696 (arguing that Congress should direct the DHS to enact regulations to govern the searches of electronic devices at the border).

[99] *See* Nicole Kolinski, Note, United States v. Arnold*: Legally Correct but Logistically Impractical*, 6 J.L. ECON. & POL'Y 31, 51 (2009).

out ever alerting travelers.[100] Accordingly, agency regulations should be implemented to prevent the misuse of this sensitive information.[101]

Despite the accomplishments of the existing CBP and ICE directives, more can be done to limit how border agents use digitally-acquired information.[102] Currently, information obtained from an electronic storage device can be shared with any number of government agencies that are assisting the search.[103] This is problematic because the existing regulations place no deadlines on when these assisting government agencies must destroy confiscated data.[104] Moreover, even if information is not shared with other agencies, travelers are not notified when CBP or ICE destroys copied information.[105] Perhaps the greatest problem with the directives, however, is that they fail to grant travelers any rights or benefits.[106] In other words, travelers cannot sue CBP or ICE for violating their respective directives.[107]

Rather than adding a reasonable suspicion requirement for forensic examinations of electronic storage devices, the issues associated with such searches should be addressed in restructured CBP and ICE directives.[108] The directives should provide explicit legally binding limitations regarding the use of electronically acquired information.[109] For example, the direc-

---

[100] Bret E. Rasner, Student Article, *International Travelers Beware: No Reasonable Suspicion Needed to Search Your Electronic Storage Devices at the Border*, 3 PHOENIX L. REV. 669, 677–78 (2010).

[101] Sales, *supra* note 74, at 1094 (stating that legislators may want to supplement the relatively weak Fourth Amendment protection granted to electronic storage devices).

[102] *See* Flipse, *supra* note 22, at 858–59 (discussing the limitations of the current ICE and CBP directives); Kolinski, *supra* note 99, at 48 (arguing that the existing directives on information retention are vague and afford agents "excessive discretion in dealing with . . . privileged information"); *supra* notes 21–25 and accompanying text (discussing the CBP and ICE directives).

[103] U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, *supra* note 21, at 2; Flipse, *supra* note 22, at 858.

[104] *See* U.S. CUSTOMS & BORDER PROT., *supra* note 21, at 9 (stating that assisting federal agencies "should" destroy any copies of confiscated information); U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, *supra* note 21, at 10 (stating that assisting federal agencies must certify to the ICE when copies of confiscated information are destroyed); Flipse, *supra* note 22, at 859 (discussing the limitations of the current directives).

[105] Flipse, *supra* note 22, at 859.

[106] U.S. CUSTOMS & BORDER PROT., *supra* note 21, at 9; U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, *supra* note 21, at 10; *see* Flipse, *supra* note 22, at 859 ("A disclaimer that the directives do not create any rights or guarantees that could be invoked by an individual tempers what limited assurance the policies may actually provide to the travelers.").

[107] *See* U.S. CUSTOMS & BORDER PROT., *supra* note 21, at 9; U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, *supra* note 21, at 10.

[108] *See* Flipse, *supra* note 22, at 874 (arguing for strict agency guidelines for notifying travelers when confiscated information has been copied and when it is eventually destroyed); Gilmore, *supra* note 75, at 781 (advocating for a new CBP policy mandating the timely destruction of information copied during forensic examinations).

[109] *See* Sales, *supra* note 74, at 1124 (emphasizing "'use limits,' which restrict the government's ability to share or otherwise use the information it does gather" over "'collection limits,' which restrict the government's ability to gather information in the first place").

tives could be amended to require that all data shared with other government agencies must be destroyed within a certain period of time.[110] Furthermore, to make the directives enforceable, travelers should be granted the right to sue the CBP or ICE for directive violations.[111] Restricting the CBP and ICE's use of confiscated data would aid national security efforts, by leaving the border search doctrine intact, while simultaneously safeguarding individual privacy interests.[112] Moreover, unlike the reasonable suspicion standard, restructured directives would be administratively practical because border agents would not have to make complex legal judgments at busy POEs.[113]

CONCLUSION

Rapid advances in technology have resulted in new personal privacy implications. While these questions of personal privacy must be addressed, the border search doctrine, which has remained largely intact for over two hundred years, should not be sacrificed. *In United States v. Cotterman (Cotterman III)*, the U.S. Court of Appeals for the Ninth Circuit—sitting en banc—improperly carved out a piece of the border search doctrine by establishing an impractical reasonable suspicion requirement for forensic examinations of electronic storage devices. This new requirement will make it more difficult for U.S. border agents to combat terrorism and child pornography. This Comment has argued, alternatively, that restricting the scope of forensic examinations through restructured CBP and ICE directives is a more appropriate vehicle for protecting personal privacy interests while still addressing the looming national security concerns that such border searches entail.

MICHAEL CRETA

Preferred Citation: Michael Creta, Comment, *A Step in the Wrong Direction: The Ninth Circuit Requires Reasonable Suspicion for Forensic Examinations of Electronic Storage Devices During Border Searches in* United States v. Cotterman, 55 B.C. L. REV. E. SUPP. 31 (2014), http://lawdigitalcommons.bc.edu/bclr/vol55/iss6/4/.

---

[110] *See* Flipse, *supra* note 22, at 859.

[111] *Contra* U.S. CUSTOMS & BORDER PROT., *supra* note 22, at 9 (stating that the directive is an internal policy statement that does not give travelers any rights); U.S. IMMIGRATION & CUSTOMS ENFORCEMENT, *supra* note 22, at 10 (same).

[112] *See* Bector, *supra* note 77, at 716–17 (arguing that new legislation can "compromise between the strong governmental interest in protecting the borders and the privacy interests retained by individuals").

[113] *See Arnold*, 533 F.3d at 1010 (9th Cir. 2008) (citing *Ickes*, 393 F.3d at 506) (indicating that forcing border agents to make legal judgments during searches is an "unworkable standard").