BYU Law Review

Volume 2012 | Issue 2 Article 14

5-1-2012

Privacy Rights Left Behind at the Border: The Exhaustive, Exploratory Searches Effectuated in United States v. Cotterman

Aaron McKnight

Privacy Rights Left Behind at the Border: The Exhaustive, Exploratory Searches Effectuated in *United States v. Cotterman*

I. INTRODUCTION

Advances in computer technology have allowed more information to be stored digitally and have permitted a greater number of people to own a personal computer. Additionally, legal professionals increasingly use digital information as sources for evidence in criminal cases.[1] The use of computers presents new questions and problems for traditional Fourth Amendment search-and-seizure doctrines.[2] For example, does the information storage-capacity of computers, and the highly personal information stored therein heighten personal privacy interests in computers above those in traditional documents? Additionally, should the government be limited in its electronic searches of personal computers or in its ability to recover deleted or discarded information on a personal computer? Courts confronted with cases regarding searches and seizures of computers need to adequately recognize and carefully analyze the new and unique characteristics of computers, or else the courts will fail to respect the proper balance between individual citizens' privacy interests and the government's interests in enforcing the law.

In *United States v. Cotterman*,[3] the Ninth Circuit failed to recognize a proper balance of Fourth Amendment interests and erred in holding that a border search of a laptop in a forensic computer laboratory is constitutional absent reasonable suspicion.[4] The court failed to adequately weigh individual privacy interests against the government's interests in performing its Fourth Amendment reasonableness evaluation. The court also failed to recognize that a forensic search of a computer is particularly offensive. The Ninth Circuit should have recognized the distinct privacy interests that are

1. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 532 (2005).

2. *Id.* at 533.

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

4. *Id.* at 1070.

violated by a forensic computer examination and should have required reasonable suspicion.

II. FOURTH AMENDMENT RESTRICTION ON SEARCHES AND SEIZURES AND THE BORDER SEARCH DOCTRINE

The Fourth Amendment protects individuals from unreasonable searches and seizures.[5] Generally, a search or seizure is unreasonable unless government agents have probable cause that a crime has been, or is being, committed.[6] However, many exceptions to the general rule exist. For example, some searches require only reasonable suspicion of the commission of a crime,[7] which is a lower standard of proof than probable cause.[8] Other searches require no suspicion at all.[9]

The exception to the probable-cause requirement pertinent to *Cotterman* is the border-search doctrine. Two Supreme Court cases and one Ninth Circuit case have developed the border-search doctrine regarding searches of computers and whether reasonable suspicion is required. This Note discusses the basics of the border-search doctrine and these cases below.

To begin, the premise of the border-search doctrine is that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons

5. U.S. CONST. amend. IV.

6. JOSHUA DRESSLER & GEORGE C. THOMAS III, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES AND PERSPECTIVES (2010). "Probable cause exists where 'the facts and circumstances within [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed." Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (second alteration in original) (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)).

7. *See* Terry v. Ohio, 392 U.S. 1 (1968) (holding that reasonable suspicion is sufficient to justify a temporary investigatory detention and a quick search for weapons). Reasonable suspicion exists when a law enforcement officer has "specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant [the] intrusion" caused by the search or seizure. *Id.* at 21.

8. Alabama v. White, 496 U.S. 325, 330 (1990) ("Reasonable suspicion is a less demanding standard than probable cause not only in the sense that reasonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause, but also in the sense that reasonable suspicion can arise from information that is less reliable . . . .").

9. For example, searches based on the searched party's consent do not require any level of suspicion. Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973).

and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[10] The rationale for the doctrine is that border searches and seizures "are justified by the national interests of the sovereign state in preventing the entry of undesirable persons and prohibited goods."[11] Additionally, individuals have a lower expectation of privacy at the border because a reasonable person understands that she is subject to customs inspections when entering a country.[12] While the Constitution permits routine border searches and seizures without any particularized suspicion, some nonroutine searches and seizures at the border require reasonable suspicion.[13]

A. Reasonable Suspicion at the Border: Montoya de Hernandez

In *United States v. Montoya de Hernandez*, the Supreme Court held that reasonable suspicion justified detention—or temporary seizure—of a traveler "beyond the scope of a routine customs search and inspection," in which the traveler was suspected of alimentary-canal smuggling.[14] The Court rejected the Ninth Circuit's determination that a standard of proof higher than reasonable suspicion was required for a nonroutine border detention.[15] Rather, the Court concluded that reasonable suspicion was sufficient to detain a traveler based on a traditional reasonableness analysis. The Court's reasonableness analysis weighed the government's increased interest in protecting its borders from illegal drugs—particularly in light of the increase in (and difficulty of detecting) alimentary-canal smuggling[16]—against the defendant's reduced privacy interests.[17]

10. United States v. Ramsey, 431 U.S. 606, 616 (1977). See *id.* at 616–20 for further discussion.

11. Sara M. Smyth, *Searches of Computers and Computer Data at the United States Border: The Need for a New Framework Following* United States v. Arnold, 2009 U. ILL. J.L. TECH. & POL'Y 69, 73 (2009).

12. United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985); Carroll v. United States, 267 U.S. 132, 154 (1925).

13. *See* Smyth, *supra* note 11, at 73; *Montoya de Hernandez*, 473 U.S. at 538. The Supreme Court has not defined what makes a search "routine" or "nonroutine."

14. *Montoya de Hernandez*, 473 U.S. at 541. Alimentary-canal smuggling occurs when a person tries to transport drugs by swallowing balloons filled with drugs. *Id.* at 534.

15. *Id.* at 540.

16. *Id.* at 538–39.

17. *Id.* at 539–40 ("Balanced against the sovereign's interests at the border are the Fourth Amendment rights of respondent.").

While the Court in *Montoya de Hernandez* established that reasonable suspicion was sufficient for a nonroutine, temporary *seizure* of a person,[18] it explicitly refrained from holding what level of suspicion, if any, would be required for a nonroutine *search*.[19]

B. No Suspicion Necessary for a Search of a Vehicle: Flores-Montano

The Supreme Court addressed whether reasonable suspicion was required for a vehicle search at the border in *United States v. Flores-Montano*.[20] In *Flores-Montano*, the Supreme Court held that no suspicion was necessary for the government "to remove, disassemble, and reassemble a vehicle's fuel tank" at the border.[21] The Ninth Circuit had previously held that a nonroutine search required reasonable suspicion based on language from *Montoya de Hernandez*, and therefore the Court reasoned that a fuel tank search qualified for reasonable-suspicion classification.[22] However, the Supreme Court rejected the Ninth Circuit rule and reliance on classification of searches as nonroutine because "the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles."[23]

The Court then engaged in a traditional reasonableness analysis. It emphasized the government's interest in preventing drug smuggling in gas tanks,[24] and weighed those interests against the privacy interests in a vehicle. The Court reasoned that a person's expectation of privacy is lower in her gas tank than in the passenger compartment of a car; and since a person at the border cannot expect privacy in the passenger compartment of her car, she cannot expect privacy in her gas tank.[25] Finally, the Court reasoned that the search

18. As mentioned in footnote 13, the Supreme Court did not define what makes a search or seizure "routine." However, the seizure in *Montoya de Hernandez* is an example of what the Court considered "nonroutine." In *Montoya de Hernandez*, customs officials detained the defendant in the customs office for sixteen hours while waiting for the traveler to defecate. *Id*. at 535.

19. *Id*. at 541 n.4.

20. 541 U.S. 149 (2004).

21. *Id*. at 155.

22. *See id*. at 152.

23. *Id*.

24. *Id*. at 153–54. In the five-and-one-half fiscal years leading up to the case, 4,619 vehicles had been seized because of drugs hidden in the gas tank. *Id*. at 153.

25. *See id*. at 154.

was not "particularly offensive," and thus did not violate legitimate privacy rights.[26] Following this analysis, the Court held that the search was reasonable, even without reasonable suspicion.

In *Flores-Montano*, the Court "[left] open the question whether, and under what circumstances, a border search [without reasonable suspicion] might be deemed unreasonable because of the particularly offensive manner in which it is carried out."[27] However, the Court indicated that reasonable suspicion may be required where the search or seizure is "highly intrusive," and it implicates the "dignity and privacy interests of the person being searched."[28] Additionally, the cases that the Court cites in support of finding unreasonableness based on the "particularly offensive manner" of a search[29] are *Kremen v. United States*[30] and *Go-Bart Importing Co. v. United States*.[31] The searches in those cases were particularly offensive because they were "exhaustive," "general exploratory search[es]."[32]

In short, *Montoya de Hernandez* and *Flores-Montano* offered few bright-line rules to follow when determining whether reasonable suspicion is necessary for a border search or seizure. Rather than rely on categories such as "routine"[33] or "intrusive,"[34] the Supreme Court instead engaged in a traditional Fourth Amendment reasonableness test in which it weighed heightened government interests against an individual's lessened expectation of privacy at the border.[35] To require reasonable suspicion, individual privacy interests must be exceptionally high because the "balance between the interests of the Government and the privacy right of the individual is . . . struck much more favorably to the Government at the

26. *Id*. at 154 n.2.

27. *Id*. (quoting United States v. Ramsey, 431 U.S. 606, 618 n.13 (1977) (internal quotation marks omitted)).

28. *Id*. at 152.

29. *Id*. at 154 n.2 (citing *Ramsey*, 431 U.S. at 618 n.13).

30. 353 U.S. 346 (1957).

31. 282 U.S. 344 (1931).

32. United States v. Cotterman, 637 F.3d 1068, 1086 n.4 (9th Cir. 2011) (Fletcher, J., dissenting).

33. *Id*. at 1080 (majority opinion).

34. *Id*.

35. United States v. Flores-Montano, 541 U.S. 149, 154 (2004); United States v. Montoya de Hernandez, 473 U.S. 531, 539–40 (1985) ("Balanced against the sovereign's interests at the border are the Fourth Amendment rights of respondent.").

border."[36] Finally, the search may be unreasonable—absent reasonable suspicion—if the search is exhaustive and exploratory.

C. No Reasonable Suspicion for Basic Computer Searches: Arnold

In *United States v. Arnold*, the Ninth Circuit addressed whether searching a laptop at the border is reasonable. The court held that searching the digital information of a laptop was reasonable without reasonable suspicion[37] where the search consisted of the border agent clicking through some files on the laptop's desktop in the presence of the defendant.[38] The Ninth Circuit concluded that the manner of the search was not particularly offensive because the court compared the laptop to a luggage-like container (notwithstanding the storage capacity of computers), which can be searched without suspicion at the border.[39]

III. *COTTERMAN* FACTS AND PROCEDURAL HISTORY

On April 6, 2007, Howard Cotterman and his wife, Maureen, drove from Mexico to the port of entry in Lukeville, Arizona and presented themselves for admission into the United States with their United States passports.[40] The Customs and Border Protection ("CBP") officer, following standard procedure, checked the passports against the CBP electronic database and found an alert on Cotterman's passport.[41] The alert[42] notified the CBP officer that Cotterman had been convicted of "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."[43] The alert further advised the officer to be on the "lookout" for child pornography in Cotterman's possession.[44]

36. *Montoya de Hernandez*, 473 U.S. at 540.

37. United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008).

38. *Id.* at 1005.

39. *Id.* at 1009–10.

40. United States v. Cotterman, 637 F.3d 1068, 1070–71 (9th Cir. 2011).

41. *Id.* at 1071.

42. The alert "was part of Operation Angel Watch, which combats child sex tourism by flagging sex offenders who target children and frequently travel outside the United States." *Id.* at 1071 n.2.

43. *Id.* at 1071.

44. *Id.*

Due to the alert, the CBP officer detained the Cottermans for a more thorough search and contacted Immigration and Customs Enforcement ("ICE").[45] ICE agents instructed the border agents to check anything the Cottermans might have that could contain child pornography.[46] CBP officers checked Cotterman's vehicle and found two laptops, one belonging to Cotterman and one belonging to Maureen, and three digital cameras.[47] After checking the cameras and the laptops, the officers found no child pornography.[48] However, the officers could not access several password-protected files on Cotterman's laptop.[49]

Soon thereafter, two ICE agents arrived at the Lukeville Port of Entry to assist in the search.[50] These agents interviewed Cotterman, who offered to help the agents gain access to the password-protected files in his computer.[51] However, the agents refused his help because they were concerned that if Cotterman had access to his computer, he would be able to delete or hide some of the files without them knowing.[52] The ICE agents instead decided to confiscate the two laptops and one of the cameras for a forensic examination.[53] After the interview, the ICE agents released the Cottermans and took the laptops and camera to the ICE office in Tucson, Arizona for the forensic examination.[54]

The next day, the ICE forensic examiner made copies of the computers' hard drives and of the camera's memory card.[55] The forensic examiner, Agent John Owen, found nothing when he examined the camera memory card and released it that same day.[56] Agent Owen then left his examination scripts running overnight to analyze the computer hard drives.[57]

45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.* at 1071–72.
53. *Id.* at 1072.
54. *Id.*
55. *Id.*
56. *Id.*
57. *Id.*

On Sunday morning, Agent Owen began examining the laptop hard drives.[58] He found nothing on Maureen's laptop, but he found seventy-five images of child pornography in the unallocated space[59] of Cotterman's laptop.[60] Agent Owen tried to contact Cotterman but learned after two days that Cotterman had fled to Sydney, Australia.[61] Agent Owen then continued to search Cotterman's laptop, and he soon found 378 images of child pornography.[62] Many of the images depicted Cotterman sexually molesting a child.[63] Over the next few months, Agent Owen discovered hundreds more pornographic images, videos, and stories depicting children.[64]

On June 27, 2009, the United States charged Cotterman in connection with the images found on his laptop.[65] After Cotterman was extradited from Australia, he moved to suppress the evidence found on his laptop.[66] The district-court judge granted Cotterman's motion,[67] and the United States appealed.[68]

IV. THE NINTH CIRCUIT DECISION IN *COTTERMAN*

In *Cotterman*, the Ninth Circuit began its analysis by determining that the search and seizure of Cotterman's laptops fell under the border-search doctrine.[69] The court then identified three categories of inappropriate borders searches: "highly intrusive searches of a person," searches that destroy property, and searches performed in a "particularly offensive manner."[70]

58. *Id*.

59. "Unallocated space is space on the hard drive where a computer stores digital information that has been erased by the computer user or information from web sites the computer has visited." *Id*. at 1072 n.5.

60. *Id*. at 1072.

61. *Id*. at 1072–73.

62. *Id*. at 1073.

63. *Id*.

64. *Id*.

65. Cotterman was charged with "production of child pornography, transportation and shipping of child pornography, receipt of child pornography, possession of child pornography, importation of obscene material, transportation of obscene material, and unlawful flight to avoid prosecution." *Id*.

66. He moved to suppress on April 18, 2008. *Id*.

67. The district judge granted the motion and made some factual findings on February 23, 2009. *Id*.

68. The government appealed on March 19, 2009. *Id*.

69. *Id*. at 1074–79.

70. *Id*. at 1079–80.

The court quickly dismissed the first two categories and focused its analysis on the last, whether ICE performed the search in a "particularly offensive manner."[71] To determine whether the search was particularly offensive, the court addressed Cotterman's two arguments.[72]

First, Cotterman argued that the search was offensive because it was unnecessary to take the laptop to Tucson for a forensic search since he had offered to help the ICE agents gain access to the password-protected files.[73] The court rejected this argument because it determined that the ICE agents' concerns about Cotterman hiding or deleting the files were reasonable.[74] The court further doubted Cotterman's true willingness to help, given the fact that he fled the country to avoid prosecution.[75]

Cotterman's second argument was that the duration of the seizure—two days—made it particularly offensive.[76] The court analyzed this argument by considering the steps that the ICE agents took to perform their search. It concluded that the length of time that the agents had held Cotterman's laptop was reasonable because of the intensive nature of a computer-forensics search and because of Agent Owen's "reasonable diligence and speed in conducting the computer forensic examination."[77]

Overall, by concluding that the search was not particularly offensive, and in making no finding regarding the presence of reasonable suspicion,[78] the court implicitly held that reasonable suspicion was not necessary for the search to actually be reasonable under the Fourth Amendment. Thus, the court reversed the trial court's decision and denied Cotterman's motion.[79]

71. *Id*. at 1079–83.

72. *Id*. at 1080.

73. *Id*.

74. *Id*.

75. *Id*. at 1080–81.

76. *Id*. at 1082.

77. *Id*. at 1083 (internal quotation marks omitted). Agent Owen went so far as to work through both Saturday and Sunday. *See supra* Part III.

78. *Id*. at 1074.

79. *Id*. at 1084.

V. ANALYSIS

The Ninth Circuit erred in its analysis of the search in *Cotterman* and in its final holding that reasonable suspicion was not necessary. The Ninth Circuit should have engaged in a more-thorough reasonableness analysis, including the weighing of government and individual interests. Further, as part of its reasonableness analysis, the Ninth Circuit should have determined that the search in *Cotterman* was exhaustive and exploratory and therefore should have held that the search was "particularly offensive." In so doing, the court should have found that reasonable suspicion was necessary to forensically search Cotterman's computer.

The court erred because it identified three categories of inappropriate border searches[80] and created a rule that border searches are not inappropriate unless they fit within one of those three categories. The Ninth Circuit specifically based most of its opinion on the "particularly offensive" category. In following its categorical rule, the Ninth Circuit failed to perform a thorough Fourth Amendment reasonableness analysis.

The Ninth Circuit's approach was inadequate because proper Fourth Amendment analysis does not rely on "[c]omplex balancing tests" focused on different categories of searches.[81] Rather, "[t]he permissibility of a particular law enforcement practice is judged by 'balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'"[82]

While the Ninth Circuit discussed the government's general interest in performing searches and seizures at the border,[83] it insufficiently evaluated the government's particular interest in excluding child pornography and decreasing child sex abuse. The Ninth Circuit also insufficiently addressed an individual's privacy

80. The three categories were (1) "highly intrusive searches of a person," (2) searches that destroy property, and (3) searches performed in a "particularly offensive manner." *Id.* at 1079–80.

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

82. United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (quoting United States v. Villamonte-Marquez, 462 U.S. 579, 588 (1983); Delaware v. Prouse, 440 U.S. 648, 654 (1979)).

83. *Cotterman*, 637 F.3d at 1074–79.

interests in his laptop. Furthermore, while analysis to determine whether the search was performed in a "particularly offensive manner" may be an important part of a reasonableness analysis, the Ninth Circuit failed to recognize that what makes a search "particularly offensive" is its exhaustive and exploratory nature, like the searches in *Kremen* and *Go-Bart Importing*.[84]

If the court had performed its analysis appropriately, it would have concluded that a reasonable-suspicion standard is necessary to conduct forensic computer searches at the border; an individual's privacy rights and the offensive, exhaustive nature of such searches outweigh the compelling government interest.

A. Government Interest in Excluding Child Pornography

Although the *Cotterman* court discussed the government's general interest in protecting its borders and excluding contraband,[85] the court should have discussed the government's particular interest in searching computers to discover contraband implicating child-sex crimes.[86] Because privacy interests in a personal laptop should outweigh the government's general interest in border security, the Ninth Circuit would have been better able to weigh the strong government interest in these types of searches if it had considered the true government interest of protecting against the sexual exploitation of children.

The government has a strong interest in preventing human trafficking in sex, both because of the growing problem of human trafficking and because of the vulnerability of its victims.[87] To illustrate, the International Labor Office estimated that in the year 2000, approximately 1.8 million children worldwide were being exploited for prostitution and pornography worldwide.[88] In response

84. *See supra* Part II.B.

85. *See supra* Part II.B.

86. Contraband found in computers may include child pornography as well as terrorist plans. Erick Lucadamo, *Reading Your Mind at the Border: Searching Memorialized Thoughts and Memories on Your Laptop and* United States v. Arnold, 54 VILL. L. REV. 541, 574 (2009) (citations omitted).

87. Hillary Clinton, *Letter from Secretary*, *in* 2011 TRAFFICKING IN PERSONS REPORT 1, *available at* http://www.state.gov/g/tip/rls/tiprpt/2011/164217.htm ("[T]he United States and the international community have made the solemn commitment to fight this scourge wherever it exists.").

88. INTERNATIONAL LABOR OFFICE, FACTS ON COMMERCIAL SEXUAL EXPLOITATION OF CHILDREN 1 (2003), *available at* http://www.wotclef.org/documents/

to this growing problem, Congress has passed laws criminalizing child-sex tourism[89] and possession and distribution of child pornography[90] to diminish the demand for commercial-sexual-exploitation of children.[91] In *New York v. Ferber*, the Supreme Court itself recognized that the reasons for prohibiting possession and distribution of child pornography are compelling.[92] Because the government has a compelling interest in prohibiting possession and distribution of child pornography, the government has a compelling interest in excluding child pornography from admittance into the United States. Thus, the government has an interest in searching computers to discover child pornography as computers enter the country.

B. Individual's Expectation of Privacy in Laptops

Additionally, the *Cotterman* court failed to adequately address an individual's privacy interests in his laptop.[93] In addressing individual privacy interests, the Ninth Circuit merely cited *Arnold* and failed to adequately discuss the unusually high privacy interest that individuals maintain in their computers.

A quick discussion of computer characteristics and use reveals why individual privacy interests in computers are so high. Computers are distinctly different from traditional "papers and effects" protected by the Fourth Amendment.[94] For example, computers made in 2005 have storage capacities equivalent to about forty-million pages of text.[95] Because of such vast storage capability, computers hold almost infinite personal information and "should not be grouped with . . . wallets, purses, luggage, and other simple containers."[96]

fs_sexualexploit_0303.pdf.

89. Child-sex tourism occurs when a person travels to a foreign country for the purpose of engaging in sex with a child. *See* U.S. DEP'T OF HOMELAND SEC., FACT SHEET: OPERATION PREDATOR—TARGETING CHILD EXPLOITATION AND SEXUAL CRIMES (Nov. 19, 2008), http://www.ice.gov/news/library/factsheets/predator.htm.

90. *See, e.g.*, 18 U.S.C. § 2252 (2006).

91. *See* U.S. DEP'T OF STATE, PREVENTION: FIGHTING SEX TRAFFICKING BY CURBING DEMAND FOR PROSTITUTION (June 27, 2011), http://www.state.gov/g/tip/rls/fs/2011/167224.htm.

92. *See* New York v. Ferber, 458 U.S. 747, 756–64 (1982).

93. *See supra* Part IV.

94. U.S. CONST. amend. IV.

95. Kerr, *supra* note 1, at 542.

96. Bret E. Rasner, Comment, *International Travelers Beware: No Reasonable Suspicion*

Searches of computers reveal far more personal information than traditional paper files. From a computer search, the government could find out what websites a person has visited and read, who the person associates with, when the person is active on the internet, and a host of other very personalized, detailed information.

Because of computers' unique characteristics, many courts and scholars have recognized the need for a "special approach" when analyzing searches and seizures of computers in general.[97] Thus, because of computers' unique capacity to store information, an individual's privacy interests invoked by a forensic search should be distinguished from other cases that reject a reasonable expectation of privacy; the court should hold that a forensic search implicates the "dignity and privacy interests of the person being searched."[98]

For example, the traditional lack of expectation of privacy in a vehicle,[99] as discussed in *Flores-Montano*,[100] is clearly distinguishable from the expectation of privacy in computers. Because of the massive amount of intimate information computers store, searches of computers threaten "dignity and privacy interests"[101] more than searches of cars.

Notwithstanding such a high expectation of privacy in a computer, *Arnold* recognized that "a search which occurs in an otherwise ordinary manner, is . . . [not unreasonable] simply due to the storage capacity of the object being searched."[102] Therefore, even the particularly high privacy interests in a laptop are not, by themselves, sufficient to make unreasonable a border search of a computer. However, a search that does not occur in an ordinary manner, but that is particularly offensive, would tip the scale towards finding an unreasonable search.

Needed to Search Your Electronic Storage Devices at the Border, 3 PHX. L. REV. 669, 697 (2010); *see also* S. 3612, 110th Cong. § 2(4) (2008).

97. Kerr, *supra* note 1, at 572; Smyth, *supra* note 11, at 71 (citing United States v. Carey, 172 F.3d 1268 (10th Cir. 1999); United States v. Tamura, 694 F.2d 591 (9th Cir. 1982)); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 104 (1994)).

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

99. *See* California v. Carney, 471 U.S. 386, 390–92 (1985) (discussing the decreased expectation of privacy in a vehicle because of the automobile exception).

100. *See supra* Part II.B.

101. *See id.*

102. United States v. Arnold, 533 F.3d 1003, 1010 (9th Cir. 2008).

C. Particularly Offensive Manner of Forensic Searches

The Ninth Circuit failed to perform a thorough reasonableness analysis because it merely likened the search in *Cotterman* to the manual computer search in *Arnold*, notwithstanding the significant differences between the two searches. These two searches are significantly different under a reasonableness analysis because both the process and the fruits of a forensic computer search are significantly different from those of a traditional search of documents or containers.[103]

A manual computer search, like that in *Arnold*, is similar to a traditional search of documents and containers, such as searching through stacks of papers contained in luggage or in a briefcase. Such a search is significantly limited by a law-enforcement officer's time and ability to read everything on site. In contrast, a forensic computer search involves copying a hard drive and running scripts to evaluate the information on the hard drive.[104] The duration of a forensics examination will last as long "as the analyst has to give it."[105] With a forensics search, the government could

> translate any documents in a foreign language, ensure that none of the seemingly innocuous pictures are actually encrypted messages, verify the licenses on any music or movies on the computer, review financial logs for evidence of insider trading, read email correspondence to ensure that there is no communication with known criminals—the list of possible [governmental] "concerns" is endless.[106]

Thus, forensic searches would be similar to the government making copies of every sheet in a stack of papers and having no restrictions whatsoever on the time and resources used to read through and analyze every detail found in the papers. Furthermore, as discussed in Part V.B, computers have the capacity to reveal far

103. *See* Kerr, s*upra* note 1, at 538.

104. United States v. Cotterman, 637 F.3d 1068, 1072 (9th Cir. 2011).

105. Kerr, s*upra* note 1, at 544.

106. *Cotterman*, 637 F.3d at 1086 n.5 (Fletcher, J., dissenting) (citing U.S. CUSTOMS AND BORDER PROTECTION DIRECTIVE No. 3340-049 (August 20, 2009) ("Searches of electronic devices help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations.")).

more information than most physical documents or containers. Such a search would be exhaustive, exploratory, and therefore, particularly offensive.

Overall, because of the exhaustive nature of forensic searches, the search in *Cotterman* should be distinguished from that in *Arnold*. The search in *Arnold* consisted of an agent looking at files on the computer in the presence of the defendant.[107] In contrast, the *Cotterman* search consisted of agents making copies of the hard drives and subjecting them to programming scripts that ran for hours.[108] A forensic search is far more capable of revealing vast amounts of highly personal information than the mere opening of a container or browsing of files by a human-being. Therefore, the Ninth Circuit should have concluded that the forensic search of Cotterman's computer was particularly offensive.

Although the government interest in safeguarding against child sex trafficking and child pornography is compelling, the reasonably high expectation of privacy in a computer and the exhaustive and offensive nature of a forensics search weigh in favor of requiring reasonable suspicion for forensic searches. The *Cotterman* decision permits a border agent to perform a forensics search on any computer entering the country without any sort of suspicion. Following *Cotterman*, no Fourth Amendment barrier prevents the government from forensically examining *every* computer entering the country to verify that its owner is not engaged in criminal activity of any type. Such searches would be "exhaustive," "general exploratory search[es]"[109] and would violate the Fourth Amendment's protection of individual privacy. These exhaustive searches will likely affect many more individuals, particularly considering the high rate of international travel[110] and the increasing ownership of laptops. Thus, to protect an individual's right to privacy and to avoid unreasonable, exhaustive searches, a reasonable-suspicion standard should be required to perform a computer forensics examination under the border-search doctrine.

107. *See supra* Part II.C.

108. *See supra* Part III.

109. *See supra* Part II.B.

110. On an average day, CBP processes 965,167 people entering the country. CBP, ON A TYPICAL DAY IN FISCAL YEAR 2010 (Feb. 25, 2011), http://www.cbp.gov/xp/cgov/about/accomplish/previous_year/fy10_stats/typical_day_fy2010.xml.

VI. CONCLUSION

The Ninth Circuit erred in *Cotterman* by holding that a border search of a laptop in a forensic computer laboratory is constitutional, absent reasonable suspicion. The court's analysis lacked the necessary depth, particularly regarding Cotterman's privacy expectations in his laptop. The Ninth Circuit should have concluded that the search of Cotterman's laptop was particularly offensive to privacy interests and was reasonable without a showing of reasonable suspicion. After the Ninth Circuit's holding, the government is free to perform extensive searches on any laptop entering the country for any reason, thus allowing the government access to practically infinite amounts of "information that is highly personal, confidential or even proprietary."[111]

Aaron McKnight[*]

111. Smyth, *supra* note 11, at 71.

* J.D. candidate, April 2013, J. Reuben Clark Law School, Brigham Young University.