

10-1-2009

## Suspicionless Border Seizures of Electronic Files: The Overextension of the Border Search Exception to the Fourth Amendment

Scott J. Upright

Follow this and additional works at: <https://scholarship.law.wm.edu/wmlr>



Part of the [Constitutional Law Commons](#), and the [Fourth Amendment Commons](#)

---

### Repository Citation

Scott J. Upright, *Suspicionless Border Seizures of Electronic Files: The Overextension of the Border Search Exception to the Fourth Amendment*, 51 Wm. & Mary L. Rev. 291 (2009), <https://scholarship.law.wm.edu/wmlr/vol51/iss1/7>

# SUSPICIONLESS BORDER SEIZURES OF ELECTRONIC FILES: THE OVEREXTENSION OF THE BORDER SEARCH EXCEPTION TO THE FOURTH AMENDMENT

## TABLE OF CONTENTS

INTRODUCTION .....	292
I. THE HISTORY OF THE FOURTH AMENDMENT AND THE BORDER SEARCH EXCEPTION .....	296
<i>A. The Border Search Exception</i> .....	297
<i>B. Federal Appellate Court Decisions</i> .....	300
II. THE CUSTOMS AND BORDER PROTECTION POLICY .....	302
<i>A. The Evolution of the CBP Policy</i> .....	303
<i>B. The Current CBP Policy</i> .....	304
III. SEARCH V. SEIZURE: WHAT RIGHTS ARE PROTECTED? ....	308
<i>A. The Seizure Clause and the Jacobsen Test</i> .....	308
<i>B. Search First, Seizure Second</i> .....	310
IV. IS COPYING COMPUTER FILES CONSIDERED A SEIZURE? ...	311
<i>A. The Jacobsen Test and the Seizure of         Electronic Files</i> .....	312
<i>B. Copying Electronic Files Under Katz and Berger</i> .....	315
<i>C. Copying Electronic Files and the Proper         Application of the Jacobsen Test</i> .....	316
V. ADDITIONAL PROBLEMS CREATED BY THE CBP POLICY ....	318
<i>A. A Possible Fourth Amendment Loophole</i> .....	318
<i>B. Racial and Religious Profiling</i> .....	319
<i>C. Privileged and Confidential Material</i> .....	320
VI. RECOMMENDATIONS .....	323
CONCLUSION .....	325

## INTRODUCTION

In 2007, United States customs officials detained Zak Reed nine separate times as Mr. Reed returned from visiting his in-laws in Canada.<sup>1</sup> According to Mr. Reed, on one occasion, customs officials “completely trashed” his car, questioned him for nearly three hours, and broke his son’s portable DVD player.<sup>2</sup> Mr. Reed also recalled one customs officer stating, “[W]e’re really too good to these detainees. We should treat them like we do in the desert. We should put a bag over their heads and zip tie their hands together.”<sup>3</sup> This treatment is especially shocking because Mr. Reed is a firefighter in his hometown of Toledo, Ohio, a twenty-year veteran of the Ohio National Guard, and customs officials never discovered anything incriminating during their examinations.<sup>4</sup> Ten years ago, however, Mr. Reed changed his name from Edward Eugene Reed to Zakariya Muhammad Reed, after he converted to Islam.<sup>5</sup> Following that change, Mr. Reed became the target of heightened scrutiny—including the detention of his cell phone—whenever he reentered the United States.<sup>6</sup>

Yasir Qadhi, a native Texan and a doctoral student at Yale University, has received similar treatment at the border.<sup>7</sup> In 2006,

---

1. Cynthia Bowers, *U.S. Citizens Question Terror Watch Lists*, Dec. 8, 2007, <http://www.cbsnews.com/stories/2007/12/08/eveningnews/main3595024.shtml>.

2. Matthew Rothchild, Letter to the Editor, *Muslim American Grilled at Border Over Religion*, THE PROGRESSIVE, May 9, 2007, [http://www.progressive.org/mag\\_mc050907](http://www.progressive.org/mag_mc050907).

3. *Id.*

4. Bowers, *supra* note 1. Farhana Y. Khera, the president of Muslim Advocates, testified at a Senate Judiciary Committee Hearing regarding a person that was most likely Mr. Reed. According to Ms. Khera, “A firefighter, 20-year former member of the National Guard, Gulf War veteran, and current member of the local Homeland Security Emergency Response Team in Toledo, OH has been questioned on numerous occasions since 2006 at the Detroit Ambassador Bridge while trying to visit family members in Ontario, Canada.” *Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. 134 (2008) [hereinafter *Hearing*] (testimony of Farhana Y. Khera, President & Executive Director, Muslim Advocates).

5. Bowers, *supra* note 1.

6. See *Hearing*, *supra* note 4, at 134 (testimony of Farhana Y. Khera) (describing how customs officials searched his cell phone).

7. See Ellen Nakashima, *Expanded Powers to Search Travelers at Border Detailed*, WASH. POST, Sept. 23, 2008, at A2; Tara Dooley, *Islamic Scholar, a Houston Native, Brings*

customs officials detained Mr. Qadhi, his wife, and his three children for five and a half hours while conducting a border search.<sup>8</sup> During the inspection, the officials took Mr. Qadhi's cell phone and copied all of the data it contained.<sup>9</sup> Two years later, in the spring of 2008, the FBI brought Mr. Qadhi back in for questioning regarding the contacts contained within the phone.<sup>10</sup> Mr. Qadhi was never found to be involved in anything illegal and has even served as a counter-terrorism consultant for the federal government.<sup>11</sup>

The stories of Mr. Reed and Mr. Qadhi are not isolated incidents.<sup>12</sup> In fact, the Association of Corporate Travel Executives conducted a survey in February 2008 and reported that seven percent of the executives surveyed stated "they had been subject to the seizure of a laptop or other electronic device" while reentering the country.<sup>13</sup> In July 2008, due to the growing concern over customs officials seizing electronic devices, the U.S. Bureau of Customs and Border Protection (the CBP) took the "unprecedented step" of publishing its policy.<sup>14</sup> This policy, entitled "U.S. Customs and Border Protection Policy Regarding Border Search of Information" (CBP Policy), was released in an effort to clarify the CBP's practices and procedures regarding the treatment of documents and electronic files during border inspections.<sup>15</sup> The CBP Policy appears to address

*Cultural Insight to Lectures on His Religion*, HOUS. CHRON., Oct. 8, 2005, available at [http://www.chron.com/CDA/archives/archive.mpl?id=2005\\_3909962](http://www.chron.com/CDA/archives/archive.mpl?id=2005_3909962).

8. Nakashima, *supra* note 7, at A2.

9. *Id.*

10. *Id.* A Department of Homeland Security (DHS) spokesperson refused to comment on Mr. Qadhi's specific case. The spokesperson claimed that the agency does not racially profile, but DHS has the authority to question any person entering the United States. *Id.*

11. Mr. Qadhi's profile matches that of a Muslim American described during Ms. Khera's Senate statement. According to that statement, Mr. Qadhi "has been consulted as an expert by federal government agencies, including the National Counterterrorism Center and the Department of State." *Hearing, supra* note 4, at 134-35 (testimony of Farhana Y. Khera).

12. See, e.g., Neil MacFarquhar, *Terror Fears Hamper U.S. Muslims' Travel*, N.Y. TIMES, June 1, 2006, available at [http://www.nytimes.com/2006/06/01/us/nationalspecial/01traveler.html?\\_r=2&pagewanted=1](http://www.nytimes.com/2006/06/01/us/nationalspecial/01traveler.html?_r=2&pagewanted=1).

13. *Hearing, supra* note 4, at 11 (statement of Susan K. Gurley, Executive Director, Association of Corporate Travel Executives).

14. Jayson Ahern, *Laptop Inspections Legal, Rare, Essential*, Aug. 11, 2008, [http://www.cbp.gov/xp/cgov/travel/admissibility/labtop\\_inspect.xml](http://www.cbp.gov/xp/cgov/travel/admissibility/labtop_inspect.xml).

15. Bureau of Customs and Border Protection, U.S. Customs and Border Protection Policy Regarding Border Search of Information, July 16, 2008, available at [http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search\\_authority.ctt/search\\_authority.pdf](http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf) [hereinafter

situations like Mr. Reed's and Mr. Qadhi's and reads, "in the course of every border search, CBP will protect the rights of individuals against unreasonable search and seizure."<sup>16</sup> The purpose of this Note is to illustrate that, to the contrary, the CBP Policy does not protect against unreasonable seizures. In reality, the CBP Policy authorizes the suspicionless seizure and detention of any electronic device "for a reasonable period of time to perform a thorough border search."<sup>17</sup>

The Supreme Court has recognized that only the federal government can effectively patrol America's borders and has held that customs officials may conduct suspicionless border searches at the international border under the "border search exception" to the Fourth Amendment.<sup>18</sup> This exception applies to each of the four hundred million travelers that enter or reenter the United States each year.<sup>19</sup> The Fourth and Ninth Circuit Courts of Appeals have applied the border search exception and allowed suspicionless border searches of electronic devices, but no court, nor legal scholarship, has addressed the topic of suspicionless border seizures of electronic devices or files.<sup>20</sup>

This Note will argue that, in order to properly protect the rights of travelers, the Court should limit the border search exception and return to a privacy-based interpretation of the Fourth Amendment's Seizure Clause. This privacy-based interpretation was first artic-

---

CBP Policy]. The U.S. Immigration and Customs Enforcement has a similar policy which states, "At any point during a border search, documents and electronic media, or copies thereof, may be detained for further review, either on-site at the place of detention or at an off-site location." ICE Policy System, Border Searches of Documents and Electronic Media, July 16, 2008, available at [http://www.cdt.org/security/20080716\\_ICE%20Search%20Policy.pdf](http://www.cdt.org/security/20080716_ICE%20Search%20Policy.pdf). Although many of the issues are the same, this Note will focus on only the CBP Policy.

16. CBP Policy, *supra* note 15, at 1.

17. *Id.* at 2. The CBP Policy also states, "[O]fficers may examine documents, books, pamphlets, and other printed material, as well as computers, disks, hard drives, and other electronic or digital storage devices. These examinations are part of CBP's long-standing practice and are essential to uncovering vital law enforcement information." *Id.* at 1.

18. *United States v. Ramsey*, 431 U.S. 606, 620 (1977) ("[T]he border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country.").

19. Ellen Nakashima, *Travelers' Laptops May Be Detained at Border*, WASH. POST, Aug. 1, 2008, at A1.

20. See *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005).

ulated over thirty years ago in *Katz v. United States*<sup>21</sup> and *Berger v. New York*,<sup>22</sup> when the Court acknowledged that both tangible and intangible property could be seized.<sup>23</sup> Accordingly, the *Katz/Berger* test would require government officials to develop probable cause before copying electronic files.<sup>24</sup>

This Note articulates the proper Fourth Amendment analysis that should govern border seizures of electronic files and suggests ways to improve the current CBP Policy. To accomplish this, Part I describes the history of the Fourth Amendment, the creation of the border search exception, and reviews the federal appellate courts' decisions involving suspicionless border searches. Part II analyzes the CBP Policy, whereas Part III explains how the Supreme Court determines what constitutes a reasonable search as opposed to a reasonable seizure. Part IV further examines the *Katz/Berger* test and demonstrates that even under the Court's current property-based test, the CBP Policy wrongly permits unreasonable seizures. Part V investigates additional problems that the CBP Policy does not properly address, such as racial and religious profiling and the disclosure of privileged information. Finally, Part VI analyzes proposed legislation and outlines recommendations that should be implemented in order to strike the proper balance between governmental interests and the individual property and privacy rights of travelers entering or leaving the United States. Ultimately, this Note illustrates that the CBP Policy stretches the government's authority too far. Suspicionless seizures are not within the Supreme

---

21. 389 U.S. 347 (1967).

22. 388 U.S. 41 (1967).

23. See *Katz*, 389 U.S. at 353; *Berger*, 388 U.S. at 58-59.

24. See *Katz*, 389 U.S. at 353. This Note argues for a probable cause standard instead of reasonable suspicion because the border search exception shifts the Fourth Amendment balance in the government's favor and allows government officials to conduct suspicionless searches. See *United States v. Ramsey*, 431 U.S. 606, 619 (1977). As a result, the government is given a great amount of latitude to develop probable cause during the initial border search; thus, it should be held to a higher standard of suspicion. The Supreme Court defined probable cause as follows: "If the facts and circumstances before the officer are such as to warrant a man of prudence and caution in believing that the offense has been committed, it is sufficient." *Carroll v. United States*, 267 U.S. 132, 161 (1925) (quoting *Stacey v. Emery*, 97 U.S. 642, 645 (1878)).

Court's border search exception and, thus, are unconstitutional under the Fourth Amendment.<sup>25</sup>

### I. THE HISTORY OF THE FOURTH AMENDMENT AND THE BORDER SEARCH EXCEPTION

The driving force behind the Fourth Amendment can be traced to the American Colonies and England's use of general warrants to search colonial homes for the evidence of any crime.<sup>26</sup> Accordingly, the Fourth Amendment has been described as "the one procedural safeguard in the Constitution that grew directly out of the events which immediately preceded the revolutionary struggle with England."<sup>27</sup> The Supreme Court, however, has not translated the Fourth Amendment "into a general constitutional 'right to privacy,'" but the Court has held that the amendment does protect "individual privacy against certain kinds of governmental intrusion."<sup>28</sup>

In order to determine which governmental intrusions (searches or seizures) are unconstitutional, there is a two-part reasonableness test. First, it must be "reasonable to conduct the particular search" or seizure.<sup>29</sup> Second, the search or seizure must be conducted in a reasonable manner.<sup>30</sup> Warrantless searches are "*per se* unreasonable," except under special circumstances.<sup>31</sup> For instance, at the international border, warrantless and suspicionless searches have been deemed reasonable and allowed under the border search ex-

---

25. The Fourth Amendment reads:

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.

U.S. CONST. amend. IV.

26. See *Boyd v. United States*, 116 U.S. 616, 625 (1886) ("[T]hen and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." (quoting John Adams)); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 536 (2005).

27. JACOB W. LANDYNSKI, *SEARCH AND SEIZURE AND THE SUPREME COURT* 19 (1966).

28. *Katz*, 389 U.S. at 350.

29. JOHN WESLEY HALL, 2 *SEARCH AND SEIZURE* 178 (3d ed. 2000).

30. *Id.*

31. *Katz*, 389 U.S. at 357.

ception.<sup>32</sup> This exception, however, was never meant, nor has the case law ever extended it, to allow the government to conduct warrantless and suspicionless seizures of property.<sup>33</sup>

### A. The Border Search Exception

The border search exception originated in the same Congress that passed the Fourth Amendment and, less famously, passed the Act of July 31, 1789, which allowed border officials to conduct warrantless searches of ships or vessels entering the United States.<sup>34</sup> Thus, the drafters of the Fourth Amendment foresaw a border exception to the warrant requirement.<sup>35</sup> This exception is based on the “recognized right of the sovereign to control ... who and what may enter the country.”<sup>36</sup> As a result, the exception allows customs officials to conduct warrantless searches of individuals entering the United States at the border,<sup>37</sup> or its “functional equivalent,” such as an international airport.<sup>38</sup>

Originally, the Supreme Court’s recognition of the border search exception focused on the government’s property interest in taxing imports.<sup>39</sup> Accordingly, in *Boyd v. United States* the Court stated “in the case of excisable or dutiable articles, the government has an interest in them for the payment of the duties thereon, and until such duties are paid has a right to keep them under observation, or

32. *United States v. Ramsey*, 431 U.S. 606, 619 (1977).

33. *Hearing*, *supra* note 4, at 11 (testimony of Larry Cunningham, Assistant District Attorney, Bronx District Attorney’s Office).

34. *See Carroll v. United States*, 267 U.S. 132, 150-51 (1925) (“That every collector, naval officer and surveyor, or other person specially appointed by either of them for that purpose, shall have full power and authority, to enter any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed; and therein to search for, seize, and secure any such goods, wares or merchandise.” (quoting the Act of July 31, 1789)).

35. *See Rasha Alzahabi*, Note, *Should You Leave Your Laptop at Home When Traveling Abroad?: The Fourth Amendment and Border Searches of Laptop Computers*, 41 IND. L. REV. 161, 166 (2008).

36. *Ramsey*, 431 U.S. at 620.

37. *Id.* at 617.

38. *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973) (describing a St. Louis airport after a nonstop flight from Mexico City as the “functional equivalent” of the border).

39. Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 314 (1998).

to pursue and drag them from concealment.”<sup>40</sup> The Court based this decision on the distinction between the search of a citizen’s home, where the government has little interest, and the search and seizure of goods being imported into the country, where the government has a substantial property interest in the taxing of imports.<sup>41</sup>

Nearly a century later, the Supreme Court explicitly recognized Congress’s broad power to regulate the border and prevent prohibited material from entering the country in *United States v. Ramsey*.<sup>42</sup> The Court stated:

Border searches, then, from before the adoption of the Fourth Amendment, have been considered to be “reasonable” by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause. This longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless “reasonable” has a history as old as the Fourth Amendment itself.<sup>43</sup>

In *Ramsey*, the Court determined that probable cause was not needed for a border search to occur but only addressed the border search exception.<sup>44</sup> The Supreme Court has never held that a border seizure exception to the Fourth Amendment is appropriate.<sup>45</sup>

---

40. *Boyd v. United States*, 116 U.S. 616, 624 (1886).

41. *Id.* at 624. The Court later lowered the warrant requirements on items in transit because of the temporal issues involved with obtaining a warrant for items that could easily be moved to another jurisdiction. *Carroll v. United States*, 267 U.S. 132, 153 (1925).

42. 431 U.S. 606 (1977).

43. *Id.* at 619. Since *Ramsey*, the Court has distinguished between “routine” and “nonroutine” border searches to determine which searches are constitutional. *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985). Reasonable suspicion is needed for “nonroutine” searches, such as strip searches, body cavity searches, and involuntary X-ray searches. 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, 980 (2007).

44. See *Ramsey*, 431 U.S. at 619.

45. In *Ramsey*, the Court quoted *United States v. Thirty-Seven Photographs*: “But a port of entry is not a traveler’s home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search.” *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971). This quote illustrates that the Court required customs officials to determine that material was illegal before conducting a seizure. In other words, the Court required probable cause.

The Supreme Court has, however, recognized the distinction between the seizure of a person and the seizure of property. In *Terry v. Ohio*, the Supreme Court stated that a person is seized when a government official, "by means of physical force or show of authority, has in some way restrained the liberty of a citizen."<sup>46</sup> Additionally, the Court held that such a seizure could only occur if the officer based the seizure on reasonable suspicion.<sup>47</sup> The Court, however, views the seizure of an international traveler at the border differently than the seizure of a person walking the streets of the interior United States.<sup>48</sup> This distinction is due to the border search exception and the lower expectation of privacy that a traveler has at the border compared to the expectation held by someone walking along the public streets.<sup>49</sup> As the Court noted in *United States v. Montoya de Hernandez*, "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior" and, therefore, the seizure of a person in order to conduct a border search does not require reasonable suspicion.<sup>50</sup> The border search exception permits the initial seizure of a traveler to occur without reasonable suspicion, but the exception does not allow the secondary seizure of the traveler's property without probable cause.<sup>51</sup>

Congress codified the border search exception in a number of statutes, including 19 U.S.C. § 482, which reads:

Any of the officers or persons authorized to board or search vessels may stop, search, and examine ... any vehicle, beast, or person, on which or whom he or they shall suspect there is

46. 392 U.S. 1, 19 n.16 (1968).

47. *Id.* at 21 ("And in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.").

48. *Compare id.* at 23 ("The crux of this case ... [is] whether there was justification for [the officer's] invasion of Terry's personal security by searching him for weapons in the course of that investigation."), with *United States v. 12 200-Foot Reels of Super 8mm Film*, 413 U.S. 123, 125 (1973) ("Import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations."), and *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant.").

49. *Montoya*, 473 U.S. at 539-40.

50. *Id.* at 538.

51. *Id.* at 538-41.

merchandise which is subject to duty, or shall have been introduced into the United States in any manner contrary to law, ... and if any such officer or other person so authorized shall find any merchandise on or about any such vehicle, beast, or person, or in any such trunk or envelope, which he shall have reasonable cause to believe is subject to duty, or to have been unlawfully introduced into the United States, ... he shall seize and secure the same for trial.<sup>52</sup>

This statute seemingly mirrors the Supreme Court's jurisprudence and provides federal agencies with plenary authority to conduct searches but requires "reasonable cause" for the seizure of any property.<sup>53</sup> Despite Congress's efforts to clarify the authority of the CBP, the border search exception has been challenged twice; both the Fourth and Ninth Circuit Courts of Appeals upheld the exception.<sup>54</sup>

### *B. Federal Appellate Court Decisions*

According to the Fourth and Ninth Circuits, customs officials do not need to have reasonable suspicion to search the electronic devices of travelers.<sup>55</sup> Neither court, however, analyzed whether suspicionless seizures of electronic files would fall under the border search exception to the Fourth Amendment; their decisions focused on only suspicionless searches.<sup>56</sup>

In *United States v. Ickes*, customs officials stopped Ickes at the United States-Canada border, searched his van, found child pornog-

---

52. 19 U.S.C. § 482 (2006). Congress also enacted 19 U.S.C. § 1582, which reads, "all persons coming into the United States from foreign countries shall be liable to detention and search by authorized officers or agents of the Government under such regulations." *Id.* § 1582.

53. *Id.* § 482.

54. See *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005).

55. See *Arnold*, 523 F.3d at 946; *Ickes*, 393 F.3d at 505 n.1 ("[S]earches of belongings at the border 'are reasonable simply by virtue of the fact that they occur at the border.'" (quoting *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004))).

56. In *Ickes*, the Fourth Circuit held "that the government was authorized by 19 U.S.C. § 1581(a) to search Ickes's computer and disks." *Ickes*, 393 F.3d at 505. In *Arnold*, the Ninth Circuit was "satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." *Arnold*, 523 F.3d at 946.

raphy, and arrested him.<sup>57</sup> The Fourth Circuit cited the applicable statute:

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 at any other authorized place ... and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board.<sup>58</sup>

Ickes claimed that this statute's language did not cover the search and subsequent seizure of his computer and disks.<sup>59</sup> The Fourth Circuit rejected this argument, applying a broad meaning to the statute, and declared that "[t]o hold otherwise would undermine the long-standing practice of seizing goods at the border even when the type of good is not specified in the statute."<sup>60</sup> The statute, however, sanctions the seizure of material only when it "appear[s] that a breach of the laws of the United States is being or has been committed."<sup>61</sup> Consequently, the Fourth Circuit recognized the authority of customs officials to conduct suspicionless border searches of electronic devices but remained silent regarding the seizure of such devices without probable cause.<sup>62</sup>

*United States v. Arnold* also involved the transportation of child pornography on a laptop across the border.<sup>63</sup> Arnold was arrested after customs officials searched his laptop following a trip to the Philippines.<sup>64</sup> The Ninth Circuit held that "reasonable suspicion is not needed for customs officials to search a laptop or other personal

57. *Ickes*, 393 F.3d at 502.

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

59. *Id.* at 504.

60. *Id.* The court cited three cases in support of the seizure of material in *Ickes*, but in each instance probable cause existed before the seizure occurred. See *United States v. Flores-Montano*, 541 U.S. 149, 150-51 (2004) (marijuana was seized after it was discovered during a border search of Flores-Montano's gas tank); *United States v. Roberts*, 274 F.3d 1007, 1009-10 (5th Cir. 2001) (agents found child pornography on the defendant's laptop before seizing the laptop); *United States v. Caminos*, 770 F.2d 361, 363 (3d Cir. 1985) (cocaine was seized after it was discovered during a border search).

61. 19 U.S.C. § 1581(e) (2000).

62. *Ickes*, 393 F.3d at 505.

63. 523 F.3d 941, 943 (9th Cir. 2008).

64. *Id.* at 943. The district court had ruled that the search required reasonable suspicion and declared the search of the laptop unconstitutional. That decision was reversed. *Id.* at 945.

electronic storage devices at the border.”<sup>65</sup> In this case as well, the customs officials seized the laptop and storage devices after they had discovered the pornographic images of minors on the computer.<sup>66</sup> Thus, the customs officials had probable cause before performing the seizure.<sup>67</sup> Additionally, the Ninth Circuit never discussed whether the suspicionless seizure of electronic files would be constitutional under the Fourth Amendment.

The Fourth and Ninth Circuit decisions, together with the Supreme Court’s decision in *Ramsey*, lead to one conclusion regarding the border search exception: courts have authorized only suspicionless border searches, not suspicionless seizures. Allowing government agents to seize property and electronic files without probable cause runs contrary to the authorizing statutes and overextends the border search exception, but as Part II will explain, that is exactly what the CBP Policy authorizes.

## II. THE CUSTOMS AND BORDER PROTECTION POLICY

The CBP’s policies regarding the seizure of items from international travelers have evolved over time and, in recent years, they have become more intrusive.<sup>68</sup> These changes prompted the Asian Law Society and the Electronic Frontier Foundation to sue the Department of Homeland Security under the Freedom of Information Act (FOIA), requesting the “release of agency records concerning CBP’s policies and procedures on the questioning, search, and inspection of travelers entering or returning to the United States at ports of entry.”<sup>69</sup> In response, the Department of Homeland Security released two document productions containing various manuals, memoranda, emails, and briefings regarding the CBP policies from

---

65. *Id.* at 946. The court pointed out two possible exceptions as to which the Supreme Court has not yet ruled: 1) “exceptional damage to property;” and 2) a “particularly offensive” search. *Id.* (citing *Flores-Montano*, 541 U.S. at 155-56).

66. *Id.* at 943.

67. *Id.* (describing how customs officials “found numerous images depicting what they believed to be child pornography” before seizing Arnold’s laptop).

68. Nakashima, *supra* note 7, at A2.

69. Complaint at 1-2, Asian Law Caucus, et al. v. U.S. Dept. of Homeland Sec., No. 08-0842 (N.D. Cal. Feb. 7, 2008), available at <http://www.eff.org/cases/foia-litigation-border-searches>.

2000 until 2008.<sup>70</sup> These documents illustrate a recognition amongst the CBP that the seizure of documents or electronic files requires some form of heightened suspicion—a requirement that, in practice, the current CBP policy ignores.

### *A. The Evolution of the CBP Policy*

In 2000, a Customs Directive entitled “Procedures for Examining Documents and Papers” stated that probable cause was required to seize any items and that “[a]n officer must have probable cause to believe a document or paper is subject to seizure, to copy it.”<sup>71</sup> Five years later, the CBP issued another set of guidelines for reviewing documents stating, “Seizure of ... documents requires probable cause that the documents have been altered, are counterfeit, or are otherwise evidence of a crime, or the fruit or instrumentality of a crime.”<sup>72</sup> These past policies indicate that, until recently, the CBP disallowed the seizure of travelers’ property without probable cause.

In July 2007, however, the CBP issued Interim Procedures for Border Search/Examination of Documents, Papers, and Electronic Information.<sup>73</sup> These procedures instructed that customs “officers may copy and transmit documents and information from electronic devices only where there is *reasonable suspicion* that ... the information may relate to, terrorist activities or other unlawful conduct.”<sup>74</sup> The requirement of reasonable suspicion was reiterated in an email forwarding instructions sent by the Field Office to Port Directors dated February 8, 2008.<sup>75</sup> The email informed customs agents that copying documents must be based on reasonable sus-

---

70. See Electronic Frontier Foundation, FOIA: Border Searches, <http://www.eff.org/cases/foia-litigation-border-searches> (last visited Sept. 22, 2009).

71. Commissioner of Customs, Customs Directive: Procedures for Examining Documents and Papers 3 (Feb. 4, 2000) (CBP FOIA production available at <http://www.eff.org/cases/foia-litigation-border-searches>).

72. Updated Guidelines for Returning Persons Who Present Fraudulent Documents and Disposition of the Seized Documents 3 (Jan. 14, 2005) (CBP FOIA production available at <http://www.eff.org/cases/foia-litigation-border-searches>).

73. Assistant Commissioner of the Office of Field Operations, Interim Procedures for Border Search/Examination of Documents, Papers, and Electronic Information (July 5, 2007) (CBP FOIA production available at <http://www.eff.org/cases/foia-litigation-border-searches>).

74. *Id.* at 2.

75. Email to “Port Directors” (Feb. 8, 2008, 11:32) (CBP FOIA production available at <http://www.eff.org/cases/foia-litigation-border-searches>).

picion and “documents and information from electronic devices or electronic storage media should not be reviewed longer than a ‘glance’” without reasonable suspicion.<sup>76</sup> So as recently as February 2008, the CBP still required reasonable suspicion in order for customs officials to copy or seize documents.<sup>77</sup>

### *B. The Current CBP Policy*

The current CBP policy was published in July 2008 in response to the pending FOIA lawsuit and a Senate Hearing.<sup>78</sup> On its face, the policy strengthens the suspicion requirement and requires probable cause to “seize” electronic devices or copies thereof. The policy reads:

*Detention and Review by Officers.* Officers may detain documents and electronic devices, or copies thereof, for a reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location. Except as noted in section D below, if after reviewing the information there is not probable cause to seize it, any copies of the information must be destroyed. All actions surrounding the detention will be documented by the officer and certified by the Supervisor.<sup>79</sup>

On the day the policy was published, former Secretary of Homeland Security Michael Chertoff wrote an editorial defending it and claimed, “[A]ny U.S. citizen's information that is copied to facilitate a search is retained only if relevant to a lawful purpose such as a criminal or national security investigation, and otherwise is erased.”<sup>80</sup> The problem, however, is that customs officials can act without suspicion, copy the hard drives of electronic devices, and review them for the amount of time necessary to conduct a “thorough” search. This procedure is the equivalent of a seizure without

---

76. *Id.*

77. *Id.*

78. See Complaint at 1, Asian Law Caucus, et al. v. U.S. Dep't of Homeland Sec., No. 08-0842 (N.D. Cal. Feb. 7, 2008), available at <http://www.eff.org/cases/foia-litigation-border-searches>; Hearing, *supra* note 4, at 142-43 (statement of S. Patrick Leahy, Chairman, S. Comm. on the Judiciary).

79. CBP Policy, *supra* note 15, at 2.

80. Michael Chertoff, Editorial, *Opposing View: Searches are Legal, Essential*, USA TODAY, July 16, 2008, <http://blogs.usatoday.com/oped/2008/07/opposing-view-s.html>.

probable cause. This conclusion is more evident when one considers that, under the current CBP procedures, hard drive searches can take many weeks to complete.<sup>81</sup> Furthermore, simply copying or imaging the hard drive could qualify as a seizure, “[b]ecause imaging generally requires commandeering the computer and disabling access to the computer for a matter of hours.”<sup>82</sup> Consequently, despite the probable cause language contained in the CBP Policy, in reality agents are permitted to conduct warrantless, suspicionless seizures of travelers’ electronic devices.

The CBP Policy also allows for the off-site inspection of electronic devices for a reasonable amount of time.<sup>83</sup> Recent technological advances, however, provide customs officials with the capability to conduct more efficient searches that do not require off-site detention of the computers or files.<sup>84</sup> For example, using COFEE (Computer Online Forensic Evidence Extractor), a device Microsoft developed in February 2008, customs agents could scan online evidence, decrypt passwords, and analyze a computer’s stored data on-site and receive results within minutes.<sup>85</sup>

Even if the searches remain on-site, they must still be completed within a reasonable amount of time in order to strike the proper Fourth Amendment balance.<sup>86</sup> The Supreme Court has “consistently rejected hard-and-fast time limits,” but in the realm of border searches, a few decisions provide some guidance.<sup>87</sup> In *United States v. Flores-Montano*, the Court upheld a nearly hour-long suspicionless search involving the partial disassembly of a traveler’s car

---

81. See, e.g., *United States v. Arnold*, 523 F.3d 941, 943 (9th Cir. 2008) (discussing how two weeks passed between the search of Arnold’s laptop and the issuance of an arrest warrant).

82. Kerr, *supra* note 26, at 561.

83. CBP Policy, *supra* note 15, at 2.

84. *Hearing*, *supra* note 4, at 183-85 (statement of Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation).

85. *Id.* at 183.

86. See *United States v. Place*, 462 U.S. 696, 709 (1983) (“[T]he brevity of the invasion of the individual’s Fourth Amendment interests is an important factor in determining whether the seizure is so minimally intrusive as to be justifiable.”).

87. *United States v. Montoya de Hernandez*, 473 U.S. 531, 543 (1985) (citing *United States v. Sharpe*, 470 U.S. 675 (1985)). Regarding domestic searches, the Court held in *Place* that, absent probable cause, “we have never approved a seizure of the person for the prolonged 90-minute period involved here.” *Place*, 462 U.S. at 709-10.

at the Mexican-American border.<sup>88</sup> However, in *United States v. Montoya de Hernandez*, the Court held that the sixteen-hour detention of a suspect thought to be “smuggling contraband in her alimentary canal” required reasonable suspicion.<sup>89</sup> And recently, the Second Circuit Court of Appeals ruled that it was reasonable to detain a group of Muslim-Americans, without suspicion, for nearly six hours during a border search.<sup>90</sup> Given these parameters and the constantly increasing storage space of electronic devices,<sup>91</sup> the CBP should amend the policy and order officials to complete all searches within six hours, unless the situation absolutely requires a longer search.<sup>92</sup>

During searches, the CBP Policy also authorizes customs officials to take notes summarizing the search.<sup>93</sup> Indeed, customs officers should be encouraged to take notes regarding the motivation for each border search, who was searched, and what, if anything, was found. These notes would allow the CBP to keep better records regarding whether certain individuals actually pose a threat to the United States. There must, however, be limitations placed on this reporting due to the millions of bits of information that computers and digital devices contain.<sup>94</sup> In fact, the United States District Court for the Central District of California addressed the issue of customs officials keeping records after a determination that the records are unrelated to the authorizing statute.<sup>95</sup> The court held, “Once it is determined that seized materials do not violate [the statute], no records may be made or retained which describe the content of the seized material or from which the identity of the person from whom the materials were seized may be ascertained.”<sup>96</sup>

---

88. *United States v. Flores-Montano*, 541 U.S. 149, 155 (2004).

89. 473 U.S. 531, 536, 541 (1985).

90. *Tabbaa v. Chertoff*, 509 F.3d 89, 100-01 (2d Cir. 2007).

91. The new iPod, for example, can hold up to 30,000 songs, 150 hours of video, and 25,000 pictures. Apple—iPod Classic—Features, <http://www.apple.com/ipodclassic/features.html> (last visited Sept. 22, 2009).

92. See, e.g., *United States v. Oyekan*, 786 F.2d 832, 836 (8th Cir. 1986) (holding that reasonable suspicion was necessary for a border search that lasted only four hours).

93. CBP Policy, *supra* note 15, at 1. The Supreme Court held that government officials taking notes during a search does not amount to a seizure. See *Arizona v. Hicks*, 480 U.S. 321, 324 (1987).

94. Kerr, *supra* note 26, at 542-43.

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

96. *Id.*

The CBP Policy's reporting provision can serve a very useful purpose, but the CBP must monitor which records should be retained or destroyed.

Moreover, despite its shortcomings, the CBP Policy does aid the government in preventing illegal or dangerous material from entering the country.<sup>97</sup> These items include everything from drugs and child pornography to terrorist materials and plans.<sup>98</sup> The Fourth Amendment, however, requires a balance between these reasonable government interests and the privacy and property interests of those subjected to searches or seizures.<sup>99</sup> This balance shifts at ports of entry in the government's favor because the "[g]overnment's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."<sup>100</sup> Despite this shift, professor Larry Cunningham testified before the Senate Judiciary Committee: "I am aware of no authority that would permit the government, without probable cause to believe it contains contraband, to keep a person's laptop or to copy the contents of its files."<sup>101</sup> Under the current case law, however, Professor Cunningham may be mistaken,<sup>102</sup> but this uncertainty illustrates the disagreement among scholars and the courts regarding what rights the Fourth Amendment protects—the right to privacy, property, security, or some combination thereof.<sup>103</sup>

---

97. See Ahern, *supra* note 14; Chertoff, *supra* note 80.

98. See, e.g., *Tabbaa v. Chertoff*, 509 F.3d 89, 97 (2d Cir. 2007) (quoting 6 U.S.C. § 111(b)(1) (stating that an aspect of the CBP's new "primary mission" is to "prevent terrorist attacks within the United States")); *United States v. Buntz*, No. 07-641, 2008 WL 2371211 (E.D. Pa. June 10, 2008) (denying defendant's motion to suppress child pornography found on his computer following a border search); *People v. Endacott*, 164 Cal. App. 4th 1346, 1347 (Cal. Ct. App. 2008) (holding that a border search of a laptop that contained child pornography did not violate the Fourth Amendment).

99. Glenn Sulmasy & John Yoo, *Katz and the War on Terrorism*, 41 U.C. DAVIS L. REV. 1219, 1222-24 (2008).

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

101. *Hearing*, *supra* note 4, at 11 (testimony of Larry Cunningham).

102. See *Arizona v. Hicks*, 480 U.S. 321, 324 (1987) ("[T]he mere recording of the serial numbers did not constitute a seizure.").

103. Clancy, *supra* note 39, at 308.

### III. SEARCH V. SEIZURE: WHAT RIGHTS ARE PROTECTED?

The Supreme Court's interpretation of the exact freedoms that the Fourth Amendment protects has evolved over time and continues to arouse debate among legal scholars.<sup>104</sup> The Court's current jurisprudence involves a bifurcation of the Fourth Amendment where the Search Clause protects privacy rights and the Seizure Clause protects property rights.<sup>105</sup>

#### A. *The Seizure Clause and the Jacobsen Test*

The Court originally based its interpretation of the Fourth Amendment entirely in property rights and tied the reasonableness of both a search or a seizure to whether the government's property interest was greater than that of the property owner.<sup>106</sup> Additionally, in 1928, the Court held that the search and seizure clauses only applied to tangible items.<sup>107</sup> This property-based interpretation of the Fourth Amendment continued until the 1960s when the Court held that the Fourth Amendment also protects privacy.<sup>108</sup> The test that has endured following the Court's decision

---

104. See *id.* at 308 (describing changes in the Supreme Court's analysis over time); G. Robert McLain, Jr., Note, *United States v. Hill: A New Rule, But No Clarity for the Rules Governing Computer Searches and Seizures*, 14 GEO. MASON L. REV. 1071, 1077 (2007) ("On one side are those who believe that fundamental differences between physical and digital searches make it impossible to apply existing Fourth Amendment rules governing searches of physical containers and documents to computers and data. On the other side are those who believe that computers and computer media are best conceptualized as containers and documents, thereby allowing existing Fourth Amendment rules to be applied to computer searches.").

105. See, e.g., *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (discussing the two types of "expectations" that the Fourth Amendment protects—one expectation regarding searches and another regarding seizures).

106. Clancy, *supra* note 39, at 312 ("Beginning with *Boyd v. United States* and extending to the latter third of the twentieth century, the Supreme Court defined the interest secured by the Fourth Amendment largely in terms of property rights.").

107. *Olmstead v. United States*, 277 U.S. 438, 464 (1928) ("The [Fourth] Amendment itself shows that the search is to be of material things—the person, the house, his papers or his effects.").

108. *Warden, Maryland Penitentiary v. Hayden*, 387 U.S. 294, 304 (1967) ("The premise that property interests control the right of the Government to search and seize has been discredited.").

in *United States v. Katz* is the “expectation of privacy” test,<sup>109</sup> articulated in Justice Harlan’s concurring opinion.<sup>110</sup> Justice Harlan stated, “My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”<sup>111</sup> The Court, however, only applied the privacy standard to review the reasonableness of searches, while retaining the property standard for seizures.<sup>112</sup>

In 1984, the Court articulated the current test for what constitutes a seizure.<sup>113</sup> According to the *Jacobsen* test, the government seizes an item when there is “meaningful interference with an individual’s possessory interests.”<sup>114</sup> The language in *Jacobsen*, however, indicates that the Court wished only to expound upon what was sufficient to constitute a seizure and not what was necessary for a seizure to occur.<sup>115</sup> In other words, the Court thought that a meaningful interference with a possessory interest would meet the criteria for a seizure, but that should not be the lone test for what qualifies as a seizure. This is evident from the Court’s reasoning in *Jacobsen*. The Court stated that the definition for a seizure “follows from our oft-repeated definition of the ‘seizure’ of a person within the meaning of the Fourth Amendment.”<sup>116</sup> The reasoning behind applying the same seizure standard to both human beings and to objects is flawed, because such a standard fails to recognize the seizure of intangible items. This is an important

109. JOHN WESLEY HALL, 1 SEARCH AND SEIZURE 20-21 (3d ed. 2000).

110. Clancy, *supra* note 39, at 328-29.

111. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The *Katz* decision, however, did not completely settle the debate over the proper Fourth Amendment standard. In 1992, the Supreme Court stated in dicta that “our cases unmistakably hold that the [Fourth] Amendment protects property as well as privacy.” *Soldal v. Cook County*, 506 U.S. 56, 62 (1992).

112. *Texas v. Brown*, 460 U.S. 730, 747 (1983) (Stevens, J., concurring) (“The [Fourth] Amendment protects two different interests of the citizen—the interest in retaining possession of property and the interest in maintaining personal privacy. A seizure threatens the former, a search the latter.”).

113. *United States v. Jacobsen*, 466 U.S. 109, 113 n.5 (1984).

114. *Id.* at 113; HALL, *supra* note 109, at 27.

115. Paul Ohm, *The Olmstedian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, ¶ 27 (2008), available at <http://stlr.stanford.edu/pdf/ohm-olmstedian-seizure-clause.pdf>.

116. *Jacobsen*, 466 U.S. at 113 n.5.

distinction because intangible items can be copied and stored without much, if any, interference with a possessory interest.

### *B. Search First, Seizure Second*

One reason for the Court's focus on property interests as opposed to privacy interests when analyzing seizures is the fact that almost all seizures are predicated by a search.<sup>117</sup> Consequently, so long as the initial search was reasonable, the suspect's privacy rights have not been violated. This reasoning is echoed in the Court's development of the "plain view" doctrine, which allows officials to seize illegal material—without a warrant—as long as the material is discovered during an otherwise reasonable search.<sup>118</sup> The plain view doctrine, however, has three limitations: 1) the officer must "not violate the Fourth Amendment in arriving at the place" where the evidence is in plain view; 2) the incriminating character of the evidence must be "immediately apparent;" and 3) the officer must have the lawful right to access the evidence.<sup>119</sup>

During a customs official's routine border search, the final prong of the plain view doctrine is always satisfied due to the border search exception—the search is always deemed reasonable.<sup>120</sup> The first and second prongs, however, are only satisfied under certain circumstances. For example, if a customs official seizes a laptop for later review, as the CBP Policy allows,<sup>121</sup> the first and second prongs of this three-part test are not satisfied. In such a scenario, the incriminating evidence cannot be "immediately apparent" if the customs official has not reviewed the files in the laptop. Furthermore, the seizure of the laptop, absent probable cause, would be an action that no court has condoned under the border search exception.<sup>122</sup> On the other hand, if the laptop was searched

---

117. Ohm, *supra* note 115, at ¶ 32.

118. See *Horton v. California*, 496 U.S. 128, 134 (1990) (citing *Coolidge v. New Hampshire*, 403 U.S. 443 (1971)); PHILLIP A. HUBBART, MAKING SENSE OF SEARCH AND SEIZURE LAW: A FOURTH AMENDMENT HANDBOOK, 219-20 (2005).

119. *Horton*, 496 U.S. at 136-37.

120. *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) ("Time and again, we have stated that searches made at the border ... are reasonable simply by virtue of the fact that they occur at the border.").

121. CBP Policy, *supra* note 15, at 2.

122. *Hearing*, *supra* note 4, at 12 (testimony of Larry Cunningham).

first, illegal material was found in it, and then it was seized, that scenario would fall within the plain view doctrine. Requiring a customs official to possess probable cause before copying electronic files follows the plain view doctrine's requirements and strikes the required Fourth Amendment balance between government interests and the interests of the travelers.<sup>123</sup> This conclusion, however, relies upon one key assumption—that copying a computer file is indeed a seizure.

#### IV. IS COPYING COMPUTER FILES CONSIDERED A SEIZURE?

In 1987, the Supreme Court held in *Arizona v. Hicks* that simply copying something does not constitute a seizure.<sup>124</sup> As a result, copying information, such as a computer hard drive, has not been deemed a seizure under current Fourth Amendment analysis.<sup>125</sup> *Hicks*, however, involved a police officer simply writing down the serial numbers from a stereo system that he suspected was stolen.<sup>126</sup> The Court's holding followed the same logic as the 1928 case of *Olmstead v. United States*.<sup>127</sup> In *Olmstead*, the Court relied on a property-based standard to examine the reasonableness of a seizure and held that the Fourth Amendment applied to only tangible items.<sup>128</sup> Recently, one legal scholar stated, "The Seizure Clause is in an *Olmsteadian* holding pattern, consistently interpreted to protect only physical property rights and to regulate only the deprivation of tangible things."<sup>129</sup> Consequently, the majority of

---

123. An email sent to all Port Directors in February 2008 urged "the importance of developing the appropriate level of suspicion before conducting a search." Email to "Port Directors," *supra* note 75. So only months before the new policy was published the CBP understood that a balance had to be struck between the interests of the government and the rights of the individuals passing through customs.

124. *Arizona v. Hicks*, 480 U.S. 321 (1987).

125. Kerr, *supra* note 26, at 548.

126. *Hicks*, 480 U.S. at 323.

127. See *Olmstead v. United States*, 277 U.S. 438, 466 (1928); see also *Silverman v. United States*, 365 U.S. 505, 510-11 (1961) (citing *Olmstead* and holding that a physical invasion is required to invoke the Fourth Amendment).

128. *Olmstead*, 277 U.S. at 466 ("Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant unless there has been an official search and seizure of his person, or such seizure of his papers or his tangible material effects.").

129. Ohm, *supra* note 115, at ¶ 2.

courts have yet to recognize that copying computer files is a seizure subject to Fourth Amendment protection.<sup>130</sup>

In his dissenting opinion in *Olmstead*, Justice Brandeis, referencing the Fourth Amendment, stated that “[c]lauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world.”<sup>131</sup> Now, over eighty years since the *Olmstead* decision, this ability to adapt is even more important given our rapidly changing, technologically driven society. For example, a computer hard drive can hold over eighty gigabytes of information, which is equivalent to approximately forty million pages of text.<sup>132</sup> Although the capacity of hard drives continues to grow, the standard for what constitutes a seizure has remained the same. There is no rationale available that could equate copying a computer hard drive to writing down the serial number of a stereo system. But the *Hicks* decision remains the controlling precedent because courts continue to improperly focus on whether a “meaningful interference with an individual’s possessory interests” has occurred.<sup>133</sup>

### A. *The Jacobsen Test and the Seizure of Electronic Files*

The Supreme Court has not defined the exact meaning of one’s “possessory interest,” but thus far the phrase has been interpreted narrowly as a “binary state of possession.”<sup>134</sup> In other words, one must have physical possession of an item to have a possessory interest.<sup>135</sup> As a result, when an alleged seizure involves tangible items, the *Jacobsen* test works well.<sup>136</sup> This test, however, becomes more troublesome when intangible property, such as electronic data,

---

130. See, e.g., *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at \*2 (W.D. Wash. May 23, 2001) (holding that copying the data from a computer in Russia is not a seizure).

131. *Olmstead*, 277 U.S. at 472 (Brandeis, J., dissenting).

132. Kerr, *supra* note 26, at 542.

133. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

134. See *Maryland v. Macon*, 472 U.S. 463, 469 (1985); Ohm, *supra* note 115, at ¶ 14.

135. Ohm, *supra* note 115, at ¶ 14.

136. In the *Macon* case, the Court held that the police did not obtain possession of obscene magazines through an illegal seizure because the original owner’s possessory interest transferred from the magazines to the money paid for them during the purchase. *Macon*, 472 U.S. at 469-71.

is involved.<sup>137</sup> According to the Court, one's possessory interest remains unchanged when a copy is made because the owner still has control over the original and, thus, no seizure has occurred.<sup>138</sup>

Under this property-based interpretation, courts have determined that a seizure requires a physical dispossession and, consequently, the copying of information does not constitute a seizure.<sup>139</sup> For instance, in *United States v. Gorshkov*, a defendant accused of computer hacking claimed that the government's evidence should be excluded because the FBI illegally copied his computer files and violated his Fourth Amendment rights.<sup>140</sup> The district court was not convinced and, citing *Hicks*, held that:

the agents' act of copying the data on the Russian computers was not a seizure under the Fourth Amendment because it did not interfere with Defendant's or anyone else's possessory interest in the data. The data remained intact and unaltered. It remained accessible to Defendant and any co-conspirators or partners with whom he had shared access. The copying of the data had absolutely no impact on his possessory rights. Therefore it was not a seizure under the Fourth Amendment.<sup>141</sup>

Similarly, in *United States v. Thomas*, the Tenth Circuit Court of Appeals held that making copies of obscene material did not qualify as a seizure, basing the decision on property interests and not privacy interests.<sup>142</sup> In *Thomas*, a UPS package accidentally broke open to reveal obscene material; UPS contacted the FBI, who copied the material and sought a warrant.<sup>143</sup> The Tenth Circuit stated, "A 'seizure' is a taking of property. It involves 'a forcible or secretive dispossession.' The materials herein remained in UPS's possession

---

137. Ohm, *supra* note 115, at ¶ 7.

138. See *Arizona v. Hicks*, 480 U.S. 321, 324 (1987).

139. *Id.* See also *United States v. Soto-Teran*, 44 F. Supp. 2d 185, 191 (E.D.N.Y. 1996) (describing the photocopying of a letter during a border search as "a search beyond a routine inspection," not a seizure).

140. *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at \*1-3 (W.D. Wash. May 23, 2001).

141. *Id.* at \*3 (citations omitted).

142. *United States v. Thomas*, 613 F.2d 787, 793 (10th Cir. 1980). Additionally, see *Bills v. Aseltine*, 958 F.2d 697, 707 (6th Cir. 1992), in which the court relied on *Hicks* to hold that photographing a scene did not interfere with a possessory interest.

143. *Thomas*, 613 F.2d at 789.

and their delivery was unaffected since they were undeliverable. The materials were searched but not seized."<sup>144</sup>

Suspicionless border seizures, however, raise a different set of issues and concerns than the *Thomas* and *Gorshkov* cases because in each case probable cause was present prior to the seizure. In *Thomas*, UPS employees called the FBI after the package had ripped open to reveal the obscene material.<sup>145</sup> In *Gorshkov*, the FBI had been investigating the defendant for months for computer hacking.<sup>146</sup> The CBP Policy does not require any level of suspicion before the hard drives or files on electronic devices may be copied or seized.<sup>147</sup>

The Fifth Circuit Court of Appeals took a small step in the correct direction in *United States v. Fortna* and ruled that a heightened level of suspicion was needed for customs officials to photocopy documents.<sup>148</sup> The court held, "We do not suggest that customs agents may photocopy material inspected at the border for other than good faith, legitimate governmental purposes."<sup>149</sup> In *Fortna*, customs officials copied the documents of a suspected drug dealer but only after receiving information from an FBI informant who was working undercover with the suspect.<sup>150</sup> The Fifth Circuit stopped short of calling the photocopying a seizure, but the court correctly pointed out the need for a heightened level of suspicion.<sup>151</sup>

The Ninth Circuit Court of Appeals seemingly struck the correct balance and, in *United States v. Ziegler*, stated that the copying of a computer hard drive is a seizure.<sup>152</sup> *Ziegler*, however, addressed

---

144. *Id.* at 793 (citations omitted).

145. *Id.* at 792-93 (discussing the FBI's review of the obscene material before the copies were made).

146. *Gorshkov*, 2001 WL 1024026, at \*1 (describing how Gorshkov had demonstrated his hacking abilities to undercover agents before being arrested).

147. CBP Policy, *supra* note 15, at 2-3.

148. *United States v. Fortna*, 796 F.2d 724, 738 (5th Cir. 1986).

149. *Id.*

150. *Id.* at 727-29.

151. *Id.* at 738. The Eastern District of New York cited the *Fortna* case and applied "a reasonable suspicion standard in determining the lawfulness of the actions of border officials in closely reading and photocopying of documents." *United States v. Soto-Teran*, 44 F. Supp. 2d 185, 191 (E.D.N.Y. 1996).

152. *United States v. Ziegler*, 474 F.3d 1184, 1190 (9th Cir. 2007) ("The remaining question is whether the search of Ziegler's office and the copying of his hard drive were 'unreasonable' within the meaning of the Fourth Amendment.... [T]he government does not deny that the search and seizure were without a warrant.").

whether the search and seizure of a computer *with the consent of the employer* still required a warrant and, as a result, the statements regarding the seizure of the hard drive are dicta.<sup>153</sup> The Ninth and Fifth Circuits, nevertheless, have correctly recognized that copying a document or a computer file is different than merely conducting a preliminary search.<sup>154</sup> These decisions demonstrate that at least some courts understand the need for the Supreme Court to change its interpretation regarding the copying of electronic files.<sup>155</sup>

### *B. Copying Electronic Files Under Katz and Berger*

In order to properly protect the rights of travelers, the Supreme Court should abandon its property-based seizure standard and return to the standard it set in the *Katz* and *Berger* cases.<sup>156</sup> Both cases involved government officials recording the voices of suspects and, in each case, the Court held that the government had illegally seized the suspect's voice—equating the conversations to property in which the suspects had a privacy interest.<sup>157</sup> In *Berger*, the Court struck down a New York statute governing wiretaps, because the statute should have particularly described “the communications, conversations, or discussions *to be seized*.”<sup>158</sup> In *Katz*, the Court held that “the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements.”<sup>159</sup> These cases, decided before the *Jacobsen* and *Hicks* cases,

---

153. *Id.* at 1185, 1190 (“We must determine whether an employee has an expectation of privacy in his workplace computer sufficient to suppress images of child pornography sought to be admitted into evidence in a criminal prosecution.”).

154. In *United States v. Seljan*, the Ninth Circuit held that customs officials could read a letter without any heightened suspicion. 547 F.3d 993, 1005 (9th Cir. 2008) (“We cannot reasonably expect customs officials wholly to abandon their sensory faculties when conducting inspections under the plenary authority of a border search.”).

155. *See, e.g., Ziegler*, 474 F.3d at 1190 (describing the copying of a hard drive as both a search and seizure).

156. *See Katz v. United States*, 389 U.S. 347, 353 (1967); *Berger v. New York*, 388 U.S. 41, 58-59 (1967).

157. *See Katz*, 389 U.S. at 353; *Berger*, 388 U.S. at 58-59.

158. *Berger*, 388 U.S. at 58-59 (“We believe the statute here is equally offensive. First, as we have mentioned, eavesdropping is authorized without requiring belief that any particular offense has been or is being committed; nor that the ‘property’ sought, the conversations, be particularly described.”).

159. *Katz*, 389 U.S. at 353.

indicate that the Court intended the Fourth Amendment's Seizure Clause to apply to both intangible and tangible items.<sup>160</sup>

The copying of electronic files merits the same treatment as the oral recordings at the heart of both *Katz* and *Berger* for two reasons. First, unlike tangible property, these items can be seized without the knowledge of the owner through electronic eavesdropping techniques or computer hacking.<sup>161</sup> Second, emails and Internet chats increasingly are replacing conversations that once took place over the telephone.<sup>162</sup> But unlike phone calls, each email or Internet chat leaves a "transcript" behind that can be copied from a computer. Currently, the Supreme Court's property-based interpretation of the Fourth Amendment allows all of these transcripts to be copied from a laptop or electronic device passing through customs.<sup>163</sup> In order to provide these transcripts with the same protection afforded telephone conversations, the Supreme Court should apply the *Katz/Berger* standard to the border seizure of electronic files. As the world continues to move towards becoming a paperless society, the Supreme Court's Fourth Amendment jurisprudence must expand to once again protect intangible property.

### *C. Copying Electronic Files and the Proper Application of the Jacobsen Test*

Even if the Supreme Court continues to apply the *Jacobsen* test to the Seizure Clause, the copying of electronic files without probable cause should qualify as a meaningful interference with a possessory interest and, thus, an unreasonable seizure. This conclusion is reached through a simple application of current property law. *Black's Law Dictionary* defines property as "[t]he right to

---

160. Ohm, *supra* note 115, at ¶ 10, 14-16.

161. As Justice Brandeis wrote in 1928 in his dissenting opinion in the *Olmstead* case, "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *United States v. Olmstead*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

162. See Shira A. Scheindlin & Johnathan M. Redgrave, *Special Masters and E-Discovery: The Intersection of Two Recent Revisions to the Federal Rules of Civil Procedure*, 30 CARDOZO L. REV. 347, 355 (2008) ("For example, a typical employee at a large company will write or receive at least fifty emails per day. If that company has one hundred thousand employees, the company could be sending and receiving over 1.5 billion emails annually.").

163. See *Arizona v. Hicks*, 480 U.S. 321, 321 (1987); CBP Policy, *supra* note 15, at 2.

possess, use, and enjoy a determinate thing .... Also, termed *bundle of rights*.”<sup>164</sup> Included in this bundle of rights is the right of the owner to exclude others and the owner’s right to destroy the property, both of which courts have found to be essential to physical possession.<sup>165</sup>

The Supreme Court of New Hampshire addressed the rights to exclude and destroy in *New Hampshire v. Nelson*.<sup>166</sup> In this case, the defendant landlord took some intimate photographs from a tenant’s residence, scanned them onto his computer, and then returned the original photographs to the tenant’s apartment.<sup>167</sup> The defendant was charged with receipt of stolen property but claimed that the government could not prove that he had the “purpose to deprive” because he returned the photographs.<sup>168</sup> The New Hampshire Supreme Court did not agree, stating that “integral to ownership ... is the right to exclude others from possessing, using and enjoying a particular item of property.”<sup>169</sup> The court continued, “though the defendant returned the original photographs, he kept a computer reproduction of the captured images, without permission, and it is these images he was convicted of unlawfully retaining.”<sup>170</sup>

The same standard should apply to the government’s actions regarding the suspicionless, warrantless copying of computer files. Once a traveler’s electronic files are copied, that traveler loses the right to destroy that property because the government now controls an exact replica. Accordingly, even under the *Jacobsen* test, the copying of electronic files constitutes a seizure, subject to Fourth Amendment protection. Thus, regardless of whether a court applies a property- or privacy-based standard, copying electronic files is a seizure and is only reasonable when government officials possess probable cause.

---

164. BLACK’S LAW DICTIONARY 1252 (8th ed. 2004).

165. Lior Jacob Strahilevitz, *The Right to Destroy*, 114 YALE L.J. 781, 794 (2005).

166. 842 A.2d 83 (N.H. 2004).

167. *Id.* at 84.

168. *Id.*

169. *Id.* at 86.

170. *Id.* (“Though the medium changed from photographic paper to a computer, the photographic images themselves remained ‘property of another.’”).

## V. ADDITIONAL PROBLEMS CREATED BY THE CBP POLICY

In addition to allowing seizures without probable cause, the CBP Policy also lacks appropriate safeguards against possible government abuses. These abuses include the possibility of other government agencies using the border search exception as a loophole to avoid Fourth Amendment requirements, the use of racial and religious profiling, and the inadvertent disclosure of privileged and confidential material.

### A. A Possible Fourth Amendment Loophole

One concern is that government officials could exploit the border search exception to evade the Fourth Amendment's search and seizure requirements.<sup>171</sup> An incident involving apparent overreaching occurred in the spring of 2008 when government officials detained two British Aerospace (BAE) executives and searched their laptops and electronic equipment.<sup>172</sup> BAE has been under federal investigation for allegedly violating the Foreign Corrupt Practices Act following its involvement in an \$84 billion deal between the British and Saudi Arabian governments in 1985.<sup>173</sup> It is not known if government officials copied the executives' files, but the CBP Policy would allow them to take such action.<sup>174</sup> David Gourevitch, a white collar defense attorney, commented on the possibility of the government's use of border searches for other investigations: "It sounds like the DoJ investigators are not getting what they hoped for as quickly as they hoped .... A stop [into the U.S.] by executives is a perfect way to do that."<sup>175</sup> Although the facts of the BAE incident are unclear, it demonstrates that government officials could

---

171. *Hearing*, *supra* note 4, at 7 (statement of Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation).

172. See Sylvia Pfeifer, *BAE Executives Held as US Steps Up Arms Deal Probe*, *FIN. TIMES*, May 19, 2008, available at <http://www.ft.com/cms/s/0/1e2a74e0-253b-11dd-a14a-000077b07658.html>.

173. Vidya Ram, *BAE Burrows Into The U.S.*, June 6, 2008, [http://www.forbes.com/2008/06/03/bae-army-trucks-markets-equity-cx\\_vr\\_0603markets08.html](http://www.forbes.com/2008/06/03/bae-army-trucks-markets-equity-cx_vr_0603markets08.html).

174. CBP Policy, *supra* note 15, at 2.

175. Pfeifer, *supra* note 172.

use the border search exception to accelerate investigations and circumvent the normal Fourth Amendment safeguards.

In 1994, a New York state court tried to limit the reach of the government and held that customs officials could only seize evidence that fell within the authorizing statutes.<sup>176</sup> These federal statutes, however, grant the CBP very broad authority to search and seize anything “introduced into the United States in any manner contrary to law.”<sup>177</sup> The statutes also allow the CBP to seize “merchandise which is [clandestinely] introduced or attempted to be introduced into the United States contrary to law.”<sup>178</sup> As a result, these statutes, coupled with the CBP Policy, seemingly permit the Department of Justice and other government agencies to use the border search exception as a loophole to conduct warrantless seizures—without the necessary suspicion, and without the proper respect to the Fourth Amendment.

### *B. Racial and Religious Profiling*

Unfortunately, the stories of Mr. Reed and Mr. Qadhi that introduced this Note are not isolated incidents. Instead, their stories and others indicate a pattern of racial and religious profiling among customs officials.<sup>179</sup> No comprehensive study has been completed, but instances of customs officials singling out individuals from minority groups and repeatedly detaining them without suspicion are becoming more and more common.<sup>180</sup> In fact, such abuses led the Asian Law Caucus to file a complaint against the Department of

---

176. *People v. LePera*, 611 N.Y.S.2d 394, 398 (N.Y. App. Div. 1994)

By going further and seizing the records on behalf of the local police, the customs inspector exceeded his authority.... [T]he limited border search exception “was granted to customs officials for a particular purpose; it may not be used to circumvent the constitutional requirement of probable cause placed upon police officers.”

(quoting *People v. Esposito*, 37 N.Y.2d 156, 160 (N.Y. 1975)).

177. 19 U.S.C. § 482 (2006).

178. *Id.* § 1595a(c).

179. See MacFarquhar, *supra* note 12 (“But Muslim Americans say they are having a harder time than most, sometimes facing an intimidating maze of barriers, if not outright discrimination. Advocacy groups have taken to labeling their predicament ‘traveling while Muslim,’ and accuse the government of ignoring a serious erosion of civil rights.”).

180. See, e.g., Editorial, *The Government and Your Laptop*, N.Y. TIMES, July 10, 2008, available at [http://www.nytimes.com/2008/07/10/opinion/10thu3.html?\\_r=1](http://www.nytimes.com/2008/07/10/opinion/10thu3.html?_r=1).

Homeland Security, alleging that the actions of customs officials have raised the "concern that [travelers] are being singled out because of racial, ethnic, or religious profiling."<sup>181</sup> The Department of Homeland Security has denied any such profiling, and former Secretary Chertoff testified in a July 2008 Senate Judiciary Committee hearing that "U.S. citizens are not treated differently based upon their ethnic background, but their individualized behavior could be a basis for singling them out, or if they matched a physical description it could be a basis for singling them out."<sup>182</sup> Despite these assurances, the Director of the Muslim Advocates, Farhana Y. Khera, testified at the same Senate hearing and described the stories of many Muslim Americans who have been stopped, detained, and harassed as they tried to reenter the country.<sup>183</sup> Slight modifications to DHS and CBP policies, such as proper maintenance of the terrorist watch list and increased information-sharing among government agencies, could further the goals of law enforcement, while protecting the rights of law-abiding citizens such as those Ms. Khera described. Although these profiling allegations are reprehensible, the failures of the CBP Policy go well beyond profiling and reach a much larger segment of society.

### *C. Privileged and Confidential Material*

The shortcomings of the CBP Policy affect every traveler carrying information abroad. For instance, attorneys and businesspeople who wish to protect privileged or confidential information face very serious problems when confronted with the potential seizure of their

---

181. Complaint at 14, *Asian Law Caucus, et al. v. U.S. Dep't of Homeland Sec.*, No. 08-0842 (N.D. Cal. Feb. 7, 2008), available at <http://www.eff.org/cases/foia-litigation-border-searches>.

182. *Hearing, supra* note 4, at 57 (statement of Jayson P. Ahern, Deputy Commissioner, U.S. Customs and Border Protection).

183. *Id.* at 134. Other examples include: 1) a California businessman who had his laptop removed from his presence for more than two hours after returning from the Hajj, a religious pilgrimage to Saudi Arabia; 2) a San Francisco software engineer reported being questioned for nearly twenty hours following three trips abroad, and the customs officials inspected his laptop and took notes; 3) another California engineer had his cell phone confiscated for five months before it was returned, broken; and 4) a Muslim American, who has testified in front of Congress on ways to improve information technology in America and has received national recognition for his work on religious equality, reported being "detained whenever he reentered the country." *Id.*

laptops or electronic devices. The CBP Policy tries to address situations involving confidential documents:

If an officer suspects that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the officer must seek advice from the Associate/Assistant Chief Counsel or the appropriate U.S. Attorney's office before conducting a search of the document.<sup>184</sup>

The policy's problem, however, is that in order to determine if the content of the document contains such evidence, the customs agent must search it before turning it over to the U.S. Attorney's Office. This creates a problem for many professionals, including psychotherapists, journalists, doctors, and social workers.<sup>185</sup>

The issues confronting attorneys are two-fold as the inadvertent disclosure of client documents or work product materials raises both attorney-client privilege concerns and ethical concerns.<sup>186</sup> Regarding attorney-client privilege, jurisdictions have adopted three separate standards to determine if the privilege has been waived through an inadvertent disclosure to a third party.<sup>187</sup> In jurisdictions following a strict standard, exposing privileged information to the inspection of a customs official would destroy the privilege—perhaps exposing the attorney to a malpractice lawsuit.<sup>188</sup> For instance, the

184. CBP Policy, *supra* note 15, at 4.

185. See Lester M. Paredes III, *The Travelers' Protection Act: Be Reasonable with My Private Information and Equipment*, 45 NO. 1 CRIM. L. BULL. 1 (2009).

186. See FED. R. EVID. 502; MODEL RULES OF PROF'L CONDUCT R. 1.6 (2007).

187. Carl Pacini, et. al., *Accountants, Attorney-Client Privilege, and the Kovel Rule: Waiver Through Inadvertent Disclosure Via Electronic Communication*, 28 DEL. J. CORP. L. 893, 908-09 (2003). The first is a strict standard where any disclosure causes the document's confidentiality to be breached "thereby destroying the basis for the continued existence of the privilege." *Underwater Storage, Inc. v. U.S. Rubber Co.*, 314 F. Supp. 546, 549 (D.D.C. 1970). The second approach focuses on the client's intent; inadvertent disclosures will not normally waive privilege unless the client's intentions were to waive the privilege. *Franzel v. Kerr Mfg. Co.*, 600 N.W.2d 66, 74-75 (Mich. Ct. App. 1999). Courts following the final approach examine the circumstances surrounding the disclosure to determine if the privilege should be considered waived. *United States v. Keystone Sanitation*, 885 F. Supp. 672, 676 (M.D. Pa. 1994).

188. See, e.g., *In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989) ("To hold, as we do, that an inadvertent disclosure will waive the privilege imposes a self-governing restraint on the freedom with which organizations such as corporations, unions, and the like label documents

Northern District of Illinois has stated “when the parties to the communication themselves do not intend the communication to be confidential or do not take reasonable steps to insure and maintain its confidentiality, the privilege does not apply or is vitiated.”<sup>189</sup> Under such a standard, any attorney traveling abroad would have to take additional precautions to preserve the attorney-client privilege.

In addition to evidentiary concerns, the CBP Policy also raises ethical concerns regarding client confidentiality.<sup>190</sup> The American Bar Association’s *Model Rules of Professional Conduct* instruct that “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.”<sup>191</sup> Furthermore, Comment 16 of Rule 1.6 reads “A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer.”<sup>192</sup> As a result, in some jurisdictions a lawyer could be subject to discipline if the duty of confidentiality is breached through the border seizure of an electronic device containing confidential files.<sup>193</sup> Many law firms are responding to these legal and ethical concerns and issuing “clean’ laptops” to employees traveling out of the country.<sup>194</sup> Additionally, in an effort to avoid exposing confidential or privileged information, employees could email files back to an office server and “clean” the hard drive before returning the country.<sup>195</sup>

Privacy and privilege concerns extend beyond law firms to businesses wishing to keep trade secrets and other documents confidential. In February 2008, the Association of Corporate Travel

---

related to communications with counsel as privileged.”).

189. *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc.*, 91 F.R.D. 254, 259 (N.D. Ill. 1980).

190. See MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2007).

191. *Id.*

192. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16 (2007).

193. Leroy J. Tornquist & Christine R. Olson, *A Last Vestige of Oregon's Wild West: Oregon's Lawless Approach to Electronically Stored Information*, 45 WILLAMETTE L. REV. 161, 202 (2008).

194. Janet I. Tu, *Privacy v. Border Security: Critics Say Laptop Searches Cross the Line*, SEATTLE TIMES, July 23, 2008, [http://seattletimes.nwsource.com/html/localnews/2008067440\\_searches23m0.html](http://seattletimes.nwsource.com/html/localnews/2008067440_searches23m0.html). These laptops contain the minimum amount of information needed for the employee's trip.

195. *Id.*

Executives conducted a survey of its members and the results showed that 81 percent of respondents believed that having a laptop seized could damage a traveler's professional reputation and standing with the traveler's company.<sup>196</sup> These concerns regarding confidential material, racial and religious profiling, and exploitation of the border search exception could be redressed through litigation, but most likely they will be remedied through legislation and some simple adjustments to the CBP Policy.

## VI. RECOMMENDATIONS

The problems surrounding the CBP Policy prompted members of Congress to propose legislation to counteract some of the CBP's more intrusive procedures.<sup>197</sup> One bill, entitled the "Travelers' Privacy Protection Act of 2008" (the TPPA), attempted to take some important steps in protecting the rights of travelers, but the proposed law also overshot in certain areas and would have usurped too much power from the CBP. For instance, the TPPA stated that "a United States resident may be searched at the border only if an official of the Department of Homeland Security has a reasonable suspicion" that the citizen is violating the laws within the Department of Homeland Security's jurisdiction.<sup>198</sup> Requiring reasonable suspicion to simply search an electronic device runs afoul of the Supreme Court's longstanding recognition of the border search exception and would likely make it too difficult for customs officials to effectively protect America's ports of entry.<sup>199</sup> The TPPA did, however, define copying electronic files as a seizure of those files but required the possession of a warrant before any seizure can take place.<sup>200</sup> The warrant requirement would place an unrealistic burden on the CBP, especially as the Court has held there are

---

196. *Hearing, supra* note 4, at 11 (statement of Susan K. Gurley, Executive Director, Association of Corporate Travel Executives).

197. *See* S. 3612, 110th Cong. (2008); H.R. 7118, 110th Cong. (2008).

198. *Id.*

199. *See* *United States v. Ramsey*, 431 U.S. 606, 619 (1977); Ahern, *supra* note 14; Chertoff, *supra* note 80.

200. S. 3612, 110th Cong. (2008); H.R. 7118, 110th Cong. (2008).

exceptions to the warrant requirement when property is in transit and a warrant cannot readily be obtained.<sup>201</sup>

The proper procedure, regardless of whether the Court or Congress articulates it, should require customs officials to have probable cause before copying any files or seizing any electronic devices. This standard strikes the correct balance between the respective interests of the government and the individual. There should be, however, two exceptions to the probable cause standard. First, an exception should permit the off-site decryption of encrypted files.<sup>202</sup> The second exception would authorize the off-site analysis of electronic files containing a foreign language that needs to be translated. Nevertheless, these files should be copied only if the customs official has a reasonable suspicion that they contain illegal material. Additionally, only those files that are under reasonable suspicion should be copied, not the entire hard drive of the electronic device. All other searches should occur on-site and within a reasonable time. In *Tabbaa v. Chertoff*, the Second Circuit held that a six-hour detention at the border was reasonable.<sup>203</sup> The Supreme Court has refused to place hard parameters on border searches,<sup>204</sup> but six hours should be the ceiling for the length of detention, barring extreme circumstances. Customs officials should also be trained in a manner that will allow them to conduct necessary searches without excessive delay. Under these circumstances, customs agents have ample opportunity to develop probable cause, while recognizing that travelers should not have to endure extreme delays.

---

201. See *United States v. Place*, 462 U.S. 696, 701 (1983); *Carroll v. United States*, 267 U.S. 132, 153, 162 (1925).

202. A federal district court in Vermont has held that a defendant charged with possession of child pornography must supply prosecutors access to his password-protected laptop. See Declan McCullagh, *Judge Orders Defendant to Decrypt PGP-protected Laptop*, Feb. 26, 2009, [http://news.cnet.com/8301-13578\\_3-10172866-38.html](http://news.cnet.com/8301-13578_3-10172866-38.html) (describing the court's ruling and how customs officials discovered the illegal material but then shutdown the computer, triggering the password protection).

203. *Tabbaa v. Chertoff*, 509 F.3d 89, 100 (2nd Cir. 2007).

204. *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985) (citing *United States v. Sharpe*, 470 U.S. 675 (1985)).

## CONCLUSION

The CBP Policy authorizes the seizure of computer files and electronic devices for as long as government officials deem necessary to “perform a thorough border search.”<sup>205</sup> This policy fails to properly recognize the rights of the individual travelers entering or leaving the United States. Initially, remedying the situation will require the Court to recognize that, under either a property- or privacy-based interpretation of the Fourth Amendment, the copying of a hard drive without probable cause jeopardizes the rights of individuals. Second, the Court or Congress must reign in the Department of Homeland Security and prevent the overextension of the border search exception. The CBP has claimed that taking these files is necessary to protect the United States against terrorism and other dangers.<sup>206</sup> The border search exception, however, permits customs officials to search every traveler entering this country.<sup>207</sup> Through the border search exception the CBP has ample opportunity to conduct searches and secure the borders of the United States. Extending this exception to allow the suspicionless seizures of electronic files is contrary to the original intent of the Court’s border search doctrine and the Fourth Amendment.<sup>208</sup> This overextension threatens the privacy and property rights of every citizen traveling abroad and will only become more pervasive as technology continues to develop. As Justice Jackson stated after serving as the chief prosecutor during the Nuremberg Trials:<sup>209</sup>

[The Fourth Amendment guarantees] are not mere second-class rights but belong in the catalog of indispensable freedoms. Among deprivations of rights, none is so effective in cowing a population, crushing the spirit of the individual and putting terror in every heart. Uncontrolled search and seizure is one of

---

205. CBP Policy, *supra* note 15, at 2.

206. Chertoff, *supra* note 80.

207. See *United States v. Ramsey*, 431 U.S. 606, 620 (1977).

208. See *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 376 (1971) (requiring that material be deemed illegal during a border search before it can be seized).

209. Jenny S. Martinez, *Process and Substance in the “War on Terror,”* 108 COLUM. L. REV. 1013, 1024 n.52 (2008).

the first and most effective weapons in the arsenal of every arbitrary government.<sup>210</sup>

If the government is genuinely committed to protecting America and defeating terrorism, it cannot do so by sacrificing these indispensable freedoms.

*Scott J. Upright\**

---

210. *Brinegar v. United States*, 338 U.S. 160, 180 (1949) (Jackson, J., dissenting).

\* J.D. candidate 2010, William & Mary School of Law; B.A., B.S., 2005, The Pennsylvania State University. Many thanks to my parents, Kirby and Joyce, and my brother, Chad, for their constant love and support. This Note was written in loving memory of Agnes Keyasko.