

*UNITED STATES V. HILL: A NEW RULE, BUT NO  
CLARITY FOR THE RULES GOVERNING COMPUTER  
SEARCHES AND SEIZURES*

*G. Robert McLain, Jr.\**

INTRODUCTION

As computers have become more prevalent in American society,<sup>1</sup> their potential as sources of evidence in criminal investigations has increased. In some cases, computers have merely replaced ink and paper, serving as additional repositories for evidence of crimes like tax fraud or drug dealing. In other cases, most notoriously in the area of child pornography, the nature of the crime has expanded to fill the capabilities of computers and computer networks.<sup>2</sup> As a result, computers have become a primary source of evidence.

As sources of evidence, computers are unique. They can contain an almost incomprehensible amount and variety of data.<sup>3</sup> Analogies to physical-world sources of evidence often fail to encapsulate the salient details of how computers store and use data. For example, although computers can “contain” evidence, unlike a traditional container, the evidence is not physical. A suitcase containing laundered money is a physical container containing physical evidence; the only physical evidence a hard drive contains is magnetic charges. Similarly, computers seem to be like file cabinets, but computer data is far more complex than paper documents. Documents may be intermingled in a file cabinet, but *parts* of documents may be scattered throughout a computer’s hard drive.

---

\* George Mason University School of Law, Juris Doctor Candidate, May 2008; Articles Editor, *GEORGE MASON LAW REVIEW*, 2007-2008; University of Florida, B.A., Philosophy. I would like to thank Dana J. Lesemann of Stroz Friedberg, LLC for taking time out of an extraordinarily busy schedule to review drafts of this article, and my wife, Alison Macdonald, for her moral (and editorial) support.

<sup>1</sup> According to the U.S. Census Bureau, the number of American households with at least one computer grew from 22.8% in 1993 to 61.8% in 2003. Jennifer Cheeseman Day, Alex Janus & Jessica Davis, *Computer and Internet Use in the United States: 2003*, 1 fig.1 (2005), available at <http://www.census.gov/prod/2005pubs/p23-208.pdf>.

<sup>2</sup> See Department of Justice, Child Exploitation and Obscenity (CEOS): Child Pornography, <http://www.usdoj.gov/criminal/ceos/childporn.html> (last visited Mar. 25, 2007).

<sup>3</sup> To grasp just how much information can be stored on a modern computer, consider the following. This Note contains roughly 79,000 characters. In plain text, each character equals one byte of data. The computer on which this Note was written has a 100 gigabyte hard drive, large enough to store roughly 1.3 million copies of this Note.

Courts have struggled to interpret the Fourth Amendment in the context of computer searches, in part because the complexity of computers invites analogizing them to familiar physical-world objects.<sup>4</sup> This Note examines the Ninth Circuit's decision in *United States v. Hill*,<sup>5</sup> a case involving a search for child pornography on a suspect's computer media, to illustrate the difficulties that courts face in doing so. Part I of this Note provides a brief background of the facts of the *Hill* case, followed by an overview of traditional Fourth Amendment rules, and then a review of some of the difficulties courts encounter in attempting to apply those rules to computer searches.

Part II of this Note analyzes two of the principal holdings in *Hill*. In Part II.A, this Note demonstrates that the new rule announced in *Hill* is an ill-advised application of a paper-world rule that unnecessarily requires law enforcement officers to state an unchanging fact with every computer search warrant application, and yet fails to protect individual privacy interests in some circumstances. In Part II.B, this Note reviews the Ninth Circuit's holding in *Hill* regarding the parameters for computer searches and assesses the Ninth Circuit's computer search rules in light of *Hill* and other recent cases. Next, Part II.B discusses the technical characteristics of computer searches and demonstrates that the technical foundation of the Ninth Circuit's approach to computer searches is flawed, and follows with an explanation of some of the unintended consequences of the Ninth Circuit's computer search rules.

Part III of this Note lists the factors courts should consider in crafting Fourth Amendment rules specifically for computer searches and seizures. This Note concludes by applying those factors to generate a rule that recognizes the unique features of computer searches while staying within the bounds of existing Supreme Court precedent, and by demonstrating the doctrinal advantages of the proposed rule through an example of how the rule would work in practice.

## I. BACKGROUND

### A. *An Overview of United States v. Hill*

Justin Hill took his desktop computer in for repairs. When the repair technician found pictures on his computer that she suspected were child pornography, she called the police, and described two of the pictures to them.<sup>6</sup> Armed with the descriptions, the police obtained a warrant to search

---

<sup>4</sup> See *infra* Part I.B.

<sup>5</sup> *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006), *cert. denied*, 2007 WL 527330 (2007).

<sup>6</sup> *Hill*, 459 F.3d at 968.

the store and seize the computer.<sup>7</sup> In the meantime, however, Hill reclaimed his computer from the store.<sup>8</sup> The police obtained a second warrant, based on the same descriptions, to search Hill's house and seize "all storage media belonging to either the computer or the individual identifying himself as the defendant . . . [and] all sexually explicit images depicting minors contained in the storage media."<sup>9</sup>

The computer was never found.<sup>10</sup> However, the police seized 22 5.25-inch floppy disks, 2 CD-ROMs, 124 3.5-inch floppy disks, and 6 Zip disks.<sup>11</sup> A government expert subsequently searched the media using Guidance Software's EnCase forensic search software.<sup>12</sup> The expert found over 1,000 images of child pornography, all contained on only two of the Zip disks.<sup>13</sup>

Hill entered a conditional guilty plea, subject to his challenge of the constitutionality of the computer search.<sup>14</sup> He offered three arguments. First, Hill argued that the mere description of the two images was insufficient to establish probable cause that he possessed child pornography in violation of 18 U.S.C. § 2252A.<sup>15</sup> Second, Hill argued that the search warrant was overbroad because it allowed the government to seize all of his computer storage media without any explanation of why an on-site search of the media to determine if each individual disk could contain evidence of child pornography was not possible.<sup>16</sup> Finally, Hill argued that the search warrant was overbroad because it contained no guidance for how the off-site search of the computer media was to be conducted (e.g., a second warrant or a search protocol describing the precise search methodology in advance).<sup>17</sup>

---

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> *Id.* at 969 n.1.

<sup>11</sup> *Id.* at 969.

<sup>12</sup> *United States v. Hill*, 322 F. Supp. 2d 1081, 1091 (C.D. Cal. 2005) [hereinafter *Hill Trial*].

<sup>13</sup> *Id.*

<sup>14</sup> *Hill*, 459 F.3d at 968.

<sup>15</sup> *Id.* at 969 (reasoning that not all pictures of nude children meet the legal definition of child pornography, and some may be protected under the First Amendment). The technician described three naked children in the photographs, two of whom appeared to be pre-pubescent. *Id.* at 968-69. Because the threshold for probable cause is only "fair probability" the court held that the descriptions were adequate. *Id.* at 972. This Note does not address the court's argument on the issue.

<sup>16</sup> Appellant's Reply Brief at 3, *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006) (No. 05-50219), 2005 WL 3517841 [hereinafter Appellant's Reply Brief].

<sup>17</sup> *Id.* at 3-4.

## B. *Fourth Amendment Rules Governing Search and Seizure*

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.<sup>18</sup>

### 1. Traditional Rules

The text of the Fourth Amendment lists only persons, houses, papers and effects as things protected against unreasonable searches and seizures.<sup>19</sup> The Supreme Court has interpreted the Fourth Amendment as protecting anything in which a person has a subjective and actual expectation of privacy, so long as society recognizes that expectation of privacy as reasonable.<sup>20</sup> A search occurs when a government agent, or someone acting on behalf of the government, interferes with that expectation of privacy.<sup>21</sup> A seizure occurs when a government agent or someone acting on behalf of the government “meaningfully interferes with an individual’s possessory interests in [the] property [in question].”<sup>22</sup>

Most searches require a warrant, and searches performed in accordance with a valid warrant are presumed to be reasonable.<sup>23</sup> To obtain a valid warrant, a government agent<sup>24</sup> must provide a neutral magistrate with a sworn statement, usually in the form of an affidavit, describing as precisely as possible the place to be searched and the items or people to be seized, and their connection to a particular crime or criminal activity.<sup>25</sup> To issue a warrant, the magistrate must determine that the sworn statements establish probable cause that the items or people described bear a sufficient relationship to the criminal activity described, and will be found at the place specified.<sup>26</sup> The certainty threshold for probable cause is relatively low; probable cause is established if the sworn statements, taken as a whole,

---

<sup>18</sup> U.S. CONST. amend. IV.

<sup>19</sup> *Id.*

<sup>20</sup> See *Katz v. United States*, 389 U.S. 347 (1967). The presently accepted formulation of the rule is taken from Justice Harlan’s concurring opinion. *Id.* at 361 (Harlan, J., concurring).

<sup>21</sup> See *Skinner v. Ry. Labor Executives Ass’n*, 489 U.S. 602, 613-15 (1989). Exactly what is and is not a search can be difficult to ascertain in some situations (e.g., when a police officer squeezes a bag to determine if it contains drugs). Wherever the boundary between search and non-search is drawn, however, the computer operations described in this Note will fall within it.

<sup>22</sup> *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

<sup>23</sup> *Katz*, 389 U.S. at 356-57.

<sup>24</sup> In most cases, the applicant must be an agent of the government, although there are exceptions in some jurisdictions. See JOHN M. BURKOFF, *SEARCH WARRANT LAW DESKBOOK* § 6:2 (Mar. 2007), available at Westlaw SRCHWARLAW § 6:2.

<sup>25</sup> See *United States v. Grubbs*, 547 U.S. 90, 126 S. Ct. 1494, 1499-1500 (2006).

<sup>26</sup> See *Zurcher v. Stanford Daily*, 436 U.S. 547, 554-55 (1978).

allow a magistrate to conclude that there is a “fair probability that contraband or evidence of a crime will be found in a particular place.”<sup>27</sup>

The Fourth Amendment was designed to protect against general, exploratory warrants.<sup>28</sup> General warrants gave the bearer the right to conduct a general, exploratory search for evidence of any illegal activity, and seize any evidence found.<sup>29</sup> By contrast, the Fourth Amendment requires not only a specific description of the place to be searched, sufficient to show that the government’s agents took reasonable steps to identify the precise location, but also a “particular” description of the items to be searched for and seized.<sup>30</sup> Thus, the scope of a search is limited and defined by the particular object or objects at which it is targeted.<sup>31</sup> In cases involving child pornography—the type of evidence at issue in *Hill*—a simple statement of the type of evidence sought<sup>32</sup> is sufficient for the purposes of meeting the particularity requirement.<sup>33</sup>

The Supreme Court favors objective tests when determining whether searches executed after obtaining a warrant are valid.<sup>34</sup> On occasion, however, the Court, in finding a search unreasonable, will infer the officer’s subjective intent (e.g., if a warrant is obviously facially invalid, or the officer misled the magistrate to obtain the warrant).<sup>35</sup> On the other hand, searches conducted pursuant to a valid warrant are presumed reasonable regardless of the subjective intent of the officer conducting the search.<sup>36</sup> Finally, searches executed pursuant to a facially valid, but actually defective warrant<sup>37</sup> are presumptively reasonable, so long as the government agent executed the warrant in good faith.<sup>38</sup>

Consider, for example, a situation in which an officer armed with a warrant to search for a stolen piano intends to find heroin also. If he limits his search to places where it is objectively reasonable to believe that the piano described in the warrant could be found, his intent is irrelevant, and any contraband heroin he discovers will be admissible under the Plain View

---

<sup>27</sup> *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

<sup>28</sup> *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

<sup>29</sup> *Id.* at 84.

<sup>30</sup> *Id.*

<sup>31</sup> *See id.* For example, if a police officer obtains a warrant to search for a stolen piano at a suspect’s residence, the officer may search the basement, but cannot search the suspect’s sock drawer (unless the suspect has a very, very large sock drawer, big enough to hold a piano).

<sup>32</sup> For example, “all evidence related to possession or distribution of child pornography.”

<sup>33</sup> *See, e.g., United States v. Grimm*, 439 F.3d 1263, 1270-71 (10th Cir. 2006).

<sup>34</sup> *Horton v. California*, 496 U.S. 128, 129 (1990).

<sup>35</sup> *United States v. Leon*, 468 U.S. 897, 926 (1984).

<sup>36</sup> *Horton*, 496 U.S. at 130.

<sup>37</sup> For example, if a witness whose testimony was necessary for probable cause was later found to have lied, or if the magistrate made a non-obvious paperwork error in completing the warrant.

<sup>38</sup> *Leon*, 468 U.S. at 920-21.

Doctrine.<sup>39</sup> If, however, the officer discovers the heroin in a place no reasonable person could believe the piano could be hidden—for example, the sock drawer—the search would be unconstitutional, and the evidence potentially subject to the exclusionary rule, which prevents both direct and derivative evidence discovered as the result of unconstitutional searches from being used against a criminal defendant.<sup>40</sup>

## 2. Computer-Specific Rules

Traditional Fourth Amendment rules that work well for physical-world searches have proven difficult to adapt uniformly to the digital world. Some courts have held that the police can seize all computer media under the control of an accused so long as the evidence contained in them could not easily have been obtained by an on-site search.<sup>41</sup> But in *United States v. Hill*, the Ninth Circuit held that an explanation of why wholesale seizure is necessary must be provided in the affidavit supporting the search warrant.<sup>42</sup> Some courts have held that police can open virtually any file on a computer, at least for the purpose of a cursory check to determine if the file is covered by the warrant, because the computer's user may have attempted to hide incriminating files by changing their names or file extensions.<sup>43</sup> Others have held that a magistrate may require the police to submit a detailed search protocol<sup>44</sup> in order to comply with the Fourth Amendment's particularity requirement.<sup>45</sup> In *United States v. Carey*, perhaps the most discussed case dealing with computer searches, the Tenth Circuit adopted a "special approach" for reviewing computer searches, in which it directly considered the searching officer's subjective intent to discover evidence of a crime beyond the scope of the warrant.<sup>46</sup>

---

<sup>39</sup> For an excellent discussion of the Plain View Doctrine under *Horton* and its application to computer searches and seizures, see David J. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841 (2005).

<sup>40</sup> *Hudson v. Michigan*, 126 S. Ct. 2159, 1263-64 (2006) (discussing the current requirements for applying the exclusionary rule).

<sup>41</sup> *United States v. Upham*, 168 F.3d 532 (1st Cir. 1999).

<sup>42</sup> *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006).

<sup>43</sup> *Rosa v. Commonwealth*, 628 S.E.2d 92, 95-96 (Va. 2006).

<sup>44</sup> A search protocol is a document describing what is being searched for, and the exact methodology to be used in conducting the search.

<sup>45</sup> *In re 3817 W. West End, First Floor, Chicago, Illinois 60621*, 321 F. Supp. 2d 953 (N.D. Ill. 2004).

<sup>46</sup> *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999). The warrant in the case covered various names and ledgers related to drug dealing. *Id.* at 1272. The officer searching the computer opened a .jpg image file with a suspicious name and discovered that it contained child pornography. *Id.* at 1273. The officer continued to open suspiciously named .jpg files and discovered additional child pornography. *Id.* The Tenth Circuit admitted the first image under the Plain View Doctrine but excluded the remaining images. *Id.* at 1276.

Commentators are also divided over whether and how existing Fourth Amendment rules should apply to computer searches and seizures. For example, in a recent edition of the *Columbia Law Review*, Professor Orin Kerr argued that, “new methods of gathering digital evidence trigger a need for new legal standards.”<sup>47</sup> In a student-written response, David Ziff argued that “courts should address the novel problem of computer searches by . . . simply applying established case law that controls the search of personal documents.”<sup>48</sup> In a Fall 2005 symposium entitled “The Search and Seizure of Computers and Electronic Evidence,” hosted by the *Mississippi Law Journal*, Kerr further developed his thesis, arguing that the two-stage process of (1) searching for and seizing computers and then (2) searching for and seizing data from computers should be reflected in the warrant process, so that the physical search is bifurcated from the digital.<sup>49</sup> While Kerr argues that rule changes are necessary, he proposes changes to procedural rules, rather than to constitutional doctrine.<sup>50</sup> At the same symposium, Professor Thomas Clancy argued that, contra Kerr, “unique Fourth Amendment rules are [not] needed to regulate [computer searches].”<sup>51</sup>

Essentially, as Clancy pointed out, the debate proceeds from two seemingly mutually exclusive premises.<sup>52</sup> 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. The former propose, as in *Carey*, to mandate changes to either procedural rules or constitutional doctrine, but may fail to adequately explain how their changes can be reconciled with existing jurisprudence. The latter, with varying degrees of technical adroitness, analogize the physical world to the digital, but often are left in a position that, whatever theoretical safeguards exist, allows police to open virtually any file on the computer media they search.

Through an analysis of *United States v. Hill*, this Note establishes two principal points. First, in Part II.A, this Note shows that when probable

---

<sup>47</sup> Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 279 (2005).

<sup>48</sup> Ziff, *supra* note 39, at 842. Ziff provides a thorough discussion of how the Plain View Doctrine can potentially be used to exclude evidence resulting from an overbroad exploratory search of a hard drive.

<sup>49</sup> Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 87-90 (2005).

<sup>50</sup> *Id.*

<sup>51</sup> Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 195 (2005). Professor Clancy's article is noteworthy because it significantly expands on David Ziff's thesis by examining a broad variety of computer search-related topics and cases in light of existing Fourth Amendment jurisprudence.

<sup>52</sup> *Id.* at 196.

cause exists that evidence of a crime is contained on a computer, law enforcement officers should be allowed to seize all computer storage media that is reasonably capable of storing the evidence sought and, contra *Hill*, they should not be required to explain to a magistrate why such a seizure is necessary. Second, in Part II.B, this Note analyzes recent Ninth Circuit computer search and seizure cases and demonstrates how, at a technical level, the mechanics of computer searches undermine the legal foundations of the Ninth Circuit's computer search and seizure rules. Finally, this section highlights some of the unintended consequences of the Ninth Circuit's rules.

## II. ANALYSIS

### A. *A New Fourth Amendment Rule: Police Must Explain why Computer Storage Media Cannot be Searched On-Site*

*Hill* established a new rule that law enforcement officers must explain to a neutral magistrate why wholesale seizure of all computer storage media is necessary prior to conducting a search. This section critically assesses the new rule, and argues that the Ninth Circuit, after correctly adopting the trial court's reasoning about the unreasonableness of requiring law enforcement officers to perform on-site pre-screening searches, failed to draw the logical conclusion, and instead erroneously applied *United States v. Tamura*.<sup>53</sup> Next, this section explains why the warrant in *Hill* was overbroad, though for different reasons than the Ninth Circuit put forth, and that law enforcement officers should be limited to seizing computer media that can reasonably be believed to store the evidence sought. This section will end with a discussion of *Hudson v. Michigan* and an assessment of its impact on cases like *Hill*.

#### 1. The Holding in *Hill*

In his appeal, *Hill* argued that the warrant authorizing the search and seizure of his computer storage media was overbroad because it allowed the police to seize *all* of his computer storage media for off-site searching without explaining why an on-site search to screen out irrelevant media was impossible.<sup>54</sup> *Hill* argued that the trial court erred in upholding the wholesale seizure of his computer storage media by simply assuming that the difficulties of an on-site search were "well-known."<sup>55</sup> According to *Hill*, the

---

<sup>53</sup> *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982).

<sup>54</sup> Appellant's Reply Brief, *supra* note 16, at 3-4.

<sup>55</sup> *Id.*

police should have had to explain why an on-site search, which might have prevented the seizure of the 22 5.25-inch floppies, 2 CD-ROMS, 124 3.5-inch floppies and 4 Zip disks that did not contain evidence, was not practical.<sup>56</sup> Because the burden of proof was on the police, the showing, however minimal, was still necessary.<sup>57</sup>

The Ninth Circuit adopted much of the trial court's opinion<sup>58</sup> word-for-word.<sup>59</sup> On this aspect of the case, however, the appellate court disagreed. The trial court focused on the reasonableness of requiring the police to bring the equipment necessary to conduct an on-site search and the potential for an on-site search to unreasonably extend the length of the search.<sup>60</sup> The Ninth Circuit agreed that it would be unreasonable to require the police to bring a laptop or other computer equipment to the search scene to determine whether particular storage media contained the evidence in question. Unlike the trial court, however, the Ninth Circuit accepted Hill's argument that the prosecution had the burden of making at least a minimal showing that a wholesale seizure was made necessary by the impracticality of searching on-site.<sup>61</sup>

In doing so, the Ninth Circuit announced a new Fourth Amendment rule for computer searches and seizures: "the government must . . . demonstrate to the magistrate *factually* why such a broad search and seizure is reasonable in the case at hand . . . [T]here must be some threshold showing before the government may 'seize the haystack to search for the needle.'"<sup>62</sup> According to the Ninth Circuit, the Fourth Amendment requires that the affidavit supporting a warrant to search for digital evidence explain in advance why, when evidence may be contained on removable media, wholesale seizure of all storage media is, or at least may be, necessary. Because the supporting affidavit contained no such explanation in this case, the warrant was overbroad.<sup>63</sup>

In its analysis, the Ninth Circuit looked to its decision *United States v. Tamura*.<sup>64</sup> In *Tamura*, police armed with a warrant to search for evidence of a kickback scheme seized entire boxes of documents, containing a substantial amount of innocent material, from the suspect's office to be searched off-site, after the suspect's officer workers refused to assist in the search.<sup>65</sup> The Ninth Circuit ruled that seizing the additional documents and searching through them later violated the Fourth Amendment, and was "the kind of

---

<sup>56</sup> *Id.*

<sup>57</sup> *Id.*

<sup>58</sup> Written by Judge Kozinski, sitting by special designation.

<sup>59</sup> *Hill Trial*, 322 F. Supp. 2d 1081, 1081 (C.D. Cal. 2005).

<sup>60</sup> *Id.* at 1088-89.

<sup>61</sup> *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006).

<sup>62</sup> *Id.*

<sup>63</sup> *Id.* at 976-77.

<sup>64</sup> *United States v. Tamura*, 694 F.2d 591(9th Cir. 1982).

<sup>65</sup> *Id.* at 595.

investigatory dragnet that the Fourth Amendment was designed to prevent.”<sup>66</sup> To be legal, wholesale seizures of large amounts of intermingled documents must be justified before a neutral magistrate.<sup>67</sup> Because the evidence discovered was described in the warrant, however, the Ninth Circuit held that suppression was not an appropriate remedy.<sup>68</sup>

Essentially, the Ninth Circuit applied *Tamura*'s paper-world rule to digital evidence, treating Hill's storage media like boxes containing intermingled documents. As with *Tamura*, the Ninth Circuit declined to apply the exclusionary rule despite the warrant's defects, because the evidence discovered (i.e., child pornography) was described in the warrant.<sup>69</sup>

## 2. A Critical Analysis of the New Rule

In his appeal, Hill faulted the trial court for approving of a warrant that allowed the police to seize all of Hill's computer media without explaining why an on-site search was impractical.<sup>70</sup> The explanation was necessary, according to Hill, because the technical knowledge of the magistrate issuing the warrant was unknown, and thus without an explanation in the supporting affidavit of why technical considerations prevented an on-site search, it would not be possible to know whether the magistrate made an informed decision.<sup>71</sup>

The trial court opinion focused on Hill's suggestion that the police could have brought a laptop computer to the scene and previewed Hill's storage media to “separate the sheep from the goats.”<sup>72</sup> Using that single theory as an analytical jumping off point, the trial court likened requiring the police to bring an expert, along with the necessary computer hardware and software, to requiring the police to bring a foreign language expert when there was reason to believe that the documents sought might not be in English.<sup>73</sup> Whether such a requirement is reasonable might hinge on the circumstances of the case.<sup>74</sup> For example, if the documents were known to be in Spanish, and the police had an ample staff of Spanish-speaking officers, it might not be unreasonable to require the presence of such an officer

---

<sup>66</sup> *Id.* (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir.1980)).

<sup>67</sup> *Id.* at 595-96.

<sup>68</sup> *Id.* at 597 (stating that “[g]enerally, the exclusionary rule does not require the suppression of evidence within the scope of a warrant simply because other items outside the scope of the warrant were unlawfully taken as well”).

<sup>69</sup> *United States v. Hill*, 459 F.3d 966, 977 (9th Cir. 2006).

<sup>70</sup> Appellant's Reply Brief, *supra* note 16, at 2.

<sup>71</sup> *Id.* at 3.

<sup>72</sup> *Hill Trial*, 322 F. Supp. 2d 1081, 1088 (C.D. Cal. 2005).

<sup>73</sup> *Id.*

<sup>74</sup> *Id.*

at the search.<sup>75</sup> It would seem that under this test, as more and more police departments train officers in computer forensics, it might not be unreasonable to require the police to bring an officer with the requisite expertise. However, even if the police were to bring an expert, as the trial court correctly points out, on-site computer searches risk damage or alteration to the evidence, place an unrealistic burden on the expert to bring equipment capable of handling any and all media he or she may find, and could take an unreasonably long amount of time to complete (which could make the search more, not less, intrusive).<sup>76</sup>

The trial court made one critical mistake. It failed to expressly draw the logical conclusion from its own analysis. In essence, it argued that the problems with on-site pre-searching of computer storage media are inherent and always present, and therefore it is unreasonable to require the police to perform such searches. It should have finished its argument by expressly concluding that, if it is always unreasonable to require the police to perform on-site pre-searches of computer storage media prior to seizure, then it is equally unreasonable to require the police to explain why they are not going to perform an on-site pre-search in a particular case.

After adopting all of the trial court's reasoning regarding the impracticalities of conducting an on-site search of the computer storage media, the Ninth Circuit failed to draw the trial court's unstated conclusion. Instead, it cited a number of cases in which the supporting affidavit explained why wholesale seizure of all computer media was necessary, and then announced a new rule, viz., that such an explanation is required.<sup>77</sup> In doing so, it rejected the very conclusion, although not expressly stated, to which the trial court's analysis leads. Instead, the Ninth Circuit uses *Tamura* to discuss why wholesale seizure without an explanation as to necessity is unreasonable, and why nonetheless the evidence obtained should not be excluded.<sup>78</sup> *Tamura* does not map quite so neatly onto the facts of *Hill*. The warrant in *Tamura* did not provide for the wholesale seizure of all documents, but rather those documents containing evidence of a kick-back scheme.<sup>79</sup> The warrant in *Hill* provided for the seizure of not only child pornographic images, but also *all* storage media.<sup>80</sup> Moreover, in *Tamura* any of the boxes could have contained the evidence sought, but searching through the evidence required only time, not expertise beyond that of an ordinary law enforcement officer. In *Hill*, it is not clear that any and all storage media the police might find could contain child pornographic images, and the search did require special expertise.

---

<sup>75</sup> *Id.*

<sup>76</sup> *Id.* at 1088-89.

<sup>77</sup> *United States v. Hill*, 459 F.3d 966, 974-77 (9th Cir. 2006).

<sup>78</sup> *Id.* at 976-77.

<sup>79</sup> *United States v. Tamura*, 694 F.2d 591, 594-95 (9th Cir. 1982).

<sup>80</sup> *Hill*, 459 F.3d at 968.

The Ninth Circuit focused on the similarities between the two cases: both involved a large amount of data in which the inculpatory was intermingled with the irrelevant, and in both cases the police seized all of the data to search later. The court's discussion of *Tamura* would have been more fruitful had it focused on the *differences* between the two cases. The type of search in *Tamura* is not inherently unreasonable to conduct on-site; it is easy to imagine situations in which it might be reasonable for the police to search a large number of documents on-site. The important and unanswered question, though, is whether it is inherently unreasonable to conduct a computer search on-site. Put differently, does the trial court's finding that on-site pre-searches of computer media are so inherently unreasonable that the police ought never be required to perform them obviate the need to state that fact to a neutral magistrate?

Not all of the trial court's supporting arguments are plausible. For example, it states that:

To ensure that they could access any electronic storage medium they might find at the scene, police would have needed far more than an ordinary laptop computer. Because computers in common use run a variety of operating systems—various versions or flavors of Windows, Mac OS and Linux, to name only the most common—police would have had to bring with them a computer (or computers) equipped to read not only all of the major media types, but also files encoded by all major operating systems. Because operating systems, media types, file systems and file types are continually evolving, police departments would frequently have to modify their computers to keep them up-to-date.<sup>81</sup>

While it is true that computer technology changes rapidly, it does not necessarily follow that the police would require multiple computers running all of the various operating systems to forensically examine storage media in the field. For example, a computer using Windows XP and running Guidance Software's EnCase program<sup>82</sup> could be used to examine drives formatted with any of the major file systems<sup>83</sup> used by Linux, Windows, or Mac

---

<sup>81</sup> *Hill Trial*, 322 F. Supp. 2d 1081, 1088-89 (C.D. Cal. 2005).

<sup>82</sup> EnCase is a commercial suite of forensic software used by police departments, several federal investigative agencies, and private computer forensic firms. In general, computer forensic software aids investigators in collecting, preserving, organizing, and analyzing digital evidence. Some of the specific features of EnCase are discussed in Part II.B, *supra*. More information on EnCase can be found on the Guidance Software web site, <http://www.guidancesoftware.com/>; *see also*, STEVE BUNTING & WILLIAM WEI, ENCASE COMPUTER FORENSICS : THE OFFICIAL ENCE : ENCASE CERTIFIED EXAMINER STUDY GUIDE (Maureen Adams, ed., Wiley Publishing, Inc. 2006). For a detailed discussion of the computer forensics process, *see* EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET (Academic Press 2d ed. 2004). While this Note uses EnCase for its examples, forensic investigators rarely rely on one tool. Other options include Access Data's Forensic Tool Kit (FTK) and specialized distributions of the Linux operating system, such as e-Fense's Helix, <http://www.e-fense.com/helix>.

<sup>83</sup> Computers use file systems to store and track files, information about files, and information about available space on computer storage media. While many modern operating systems can read and write data to multiple file systems, most operating systems typically have specific file systems associ-

OS. Individual files created by specific programs might be more problematic.<sup>84</sup> Even so, the burden on any one police department to maintain a single computer running forensic software is not particularly onerous.

The existence of a wide variety of removable storage media (e.g., floppy disks) is similarly not a barrier to requiring on-site searches in most cases. Police departments could be required to maintain field kits equipped with readers for storage devices they most commonly encounter in the field. For example, to perform an on-site search in this case, the police would have needed only a 5.25-inch floppy drive, a 3.5-inch floppy drive, a CD-ROM drive, and a Zip drive.<sup>85</sup> While it is easy to imagine other cases where less common and more expensive drives might be required (e.g., in searches of businesses that use proprietary backup systems), courts could simply allow the police to seize only storage media that could not be read on location. So, the mere burden of maintaining equipment would seem not to justify, by itself, wholesale seizure of all storage media as a default rule.

The trial court's next two arguments are more persuasive. On-site searching can result in destroying or altering evidence, and can easily take so long to perform that it would place undue burdens on both the police and the suspect whose premises are being searched.<sup>86</sup> The field is far from the controlled environment of the lab.<sup>87</sup> Things as essential as the integrity of the home or office's wiring, and thus the reliability of the power supply the officer must depend on for the safe operating of the necessary equipment, are not easily ascertainable.<sup>88</sup> In order to avoid damaging or altering the original evidence, forensic experts typically create a bitstream<sup>89</sup> copy of the storage media, and then examine the copy.<sup>90</sup> The process, however, is time consuming. The police are thus placed between two untenable positions: either forgo the bitstream image and risk damaging or writing to (or worse, overwriting completely) the original storage media, or make forensically

---

ated with them. For example, Windows XP uses either the FAT32 or NTFS file systems, while Mac OS X uses HFS+ by default. *See* WARREN G. KRUSE II & JAY G. HEISER, *COMPUTER FORENSICS: INCIDENT RESPONSE ESSENTIALS* 72-77 (Addison-Wesley 2002) (discussing file systems); *see also* CASEY, *supra* note 82, at 202-04, 257-59.

<sup>84</sup> For example, most common picture file formats (.gif, .jpg, .png, .tiff, etc.) can be opened from within virtually all operating systems, and text-based files, such as Word documents, can be searched with EnCase, even on a computer that does not have the corresponding document editor installed on it. Files that create proprietary formatted databases, or encrypted files, could be more difficult to search quickly in the field.

<sup>85</sup> *See Hill*, 459 F.3d at 969.

<sup>86</sup> *Hill Trial*, 322 F. Supp. 2d at 1089.

<sup>87</sup> *Id.*

<sup>88</sup> *Id.*

<sup>89</sup> A bitstream copy (sometimes called a bit-for-bit or byte-for-byte copy) is a copy of every one-and-zero (bits). Bitstream copies are important in computer forensics because they capture deleted files and areas that operating systems treat as empty, but which can often contain evidence. *See* KRUSE & HEISER, *supra* note 83, at 14-15; *see also* CASEY, *supra* note 82, at 226, 261-64, 294-301.

<sup>90</sup> CASEY, *supra* note 82, at 225-28.

sound copies of all storage media found, review the copies to see if they contain evidence, and then take only the original storage media that corresponds to the copies that contain evidence.

The latter option is fraught with problems. First, it is unlikely that the police will know beforehand the type and quantity of the storage media that they will find, making it difficult to know what to bring for bitstream copying purposes.<sup>91</sup> Second, even if the police were adequately equipped to make the copies, the copying process takes time to perform and verify. Finally, once the copies were made, the police would have to search each copy for the evidence sought in the warrant. A simple glance at the files would not be sufficient, because evidence can be hidden or deleted, but recoverable.<sup>92</sup> This process is also time consuming, and, because both the search and any evidence found may be subject to later scrutiny, requires documentation. The police would have to be prepared to conduct a full forensic examination in the field, and the suspect would have the inconvenience of having the police in his home or office while they did it.

In most cases, then, it is not reasonable to require the police to conduct an on-site pre-search of storage media, and, in many cases such a search would be unreasonable. Although some exceptions may exist, for example, cases in which the suspect has only a few CD-ROMs, it is unlikely that the police will know, at the time they seek a warrant, what type and quantity of media they will encounter.

Thus, computer storage media differs in an important regard from the boxes of paper documents in *Tamura*: by its nature, digital evidence on computer storage media is almost always better suited to an off-site search by an expert in a controlled environment.<sup>93</sup> This proposition is not fact-sensitive, and is true regardless of the magistrate's technical knowledge.<sup>94</sup> By requiring the police to explain why a wholesale seizure of all storage media is necessary, the Ninth Circuit requires the police to explain the same general and unchanging fact to each magistrate with every warrant request, rather than requiring an explanation in the exceptional case where an on-site search—which carries with it its own complications—will be used.

Finally, as the trial court noted:

Search warrants must be specific. 'Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals

---

<sup>91</sup> The police would not, however, have to bring a floppy disk for each floppy, or a CD-R for each CD-ROM. It is possible to make a bitstream copy of lower capacity storage media (such as a floppy disk) and store it as a file (usually called an "image file" or "forensic image") on a larger capacity disk (such as a hard drive). For example, a single 300 Gigabyte drive would have accommodated all of the storage media found at Hill's home.

<sup>92</sup> CASEY, *supra* note 82, at 225.

<sup>93</sup> *Id.*

<sup>94</sup> In this regard, computer forensics is somewhat like DNA analysis. Regardless of the facts of any particular case, both are better suited to the laboratory than the field.

with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.<sup>95</sup>

The Ninth's Circuit's new rule addresses neither. The warrant, as written, was as particular as it could be, given the circumstances. Hill challenged the breadth of the warrant.<sup>96</sup> The question, then, was whether probable cause existed to believe that child pornography would be found on Hill's computer storage media. The mechanism of a search can bring it outside of a warrant, but it cannot erase the existence of probable cause.

B. *Perpetuating a Myth: Changed File Extensions, Search Methods, and Fourth Amendment Rules*

The Ninth Circuit missed an opportunity to clarify the rules surrounding computer searches in *Hill*. The factual circumstances of the case were ideal. The police obtained a warrant to search for child pornography, which the defendant undoubtedly possessed.<sup>97</sup> The defendant did not claim that the images were not his, or that he had been harmed by the search in some way other than having his collection of contraband images discovered.<sup>98</sup> The Ninth Circuit should have announced new, clear guidelines for computer searches. Even if their new rule invalidated the search warrant, the Ninth Circuit could simply have applied *Hudson v. Michigan*<sup>99</sup> to prevent the evidence from being excluded.<sup>100</sup> Instead, they narrowly interpreted the defendant's objection to the lack of an explicit search methodology, then relied on the often-used but technically flawed assertion that computer users' ability to change file names and extensions requires allowing the police to "ex-

---

<sup>95</sup> *Hill Trial*, 322 F. Supp. 2d 1081, 1087 (C.D. Cal. 2005) (citing *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993)).

<sup>96</sup> Appellant's Reply Brief, *supra* note 16, at 2.

<sup>97</sup> *United States v. Hill*, 459 F.3d 966, 968-69 (9th Cir. 2006).

<sup>98</sup> *Id.*

<sup>99</sup> 126 S. Ct. 2159 (2006).

<sup>100</sup> Despite Justice Scalia's assertions to the contrary, *Hudson* is a significant limitation on the exclusionary rule. The Court established the two conditions for applying the exclusionary rule: (1) the violation of the Fourth Amendment must be an unattenuated but-for cause of the discovery of the evidence; and (2) the deterrence benefit of excluding the evidence must "outweigh its substantial social costs." *Id.* at 2164-65. In a case like *Hill* it would be virtually impossible get evidence excluded solely because the warrant was overbroad. Assume, for example, that the police had unreasonably seized a stack of punch cards from Hill. If no child pornography were found, a Fourth Amendment violation would exist, but would not be a but-for cause of finding any other evidence. If, by some miracle, child pornography were found, it would be much harder to say that the punch cards could not reasonably be believed to contain child pornography, thus eliminating the Fourth Amendment violation. Even if a court found that the cards could not be reasonably believed to contain child pornography, the court would balance the strong social interest in convicting collectors of child pornography against the minimal deterrence effect of suppression on innocent police behavior.

amine” every file on a computer. In doing so, the Court perpetuated a myth that justifies allowing the police to open any file on a computer while conducting a search.

This section first presents the argument and holding in *Hill* regarding the limits of computer searches, then analyzes the permissible scope of computer searches under *Hill* and *United States v. Adjani*,<sup>101</sup> another recent Ninth Circuit case. Next, this section critically assesses the validity of the Ninth Circuit’s computer search rules in light of how computer searches are actually conducted. Finally, this section examines some problematic consequences of the Ninth Circuit’s computer search rules.

### 1. The Argument and Holding in *Hill*

In addition to attacking the wholesale seizure of his computer disks, Hill argued that the warrant was overbroad because it contained a “complete absence of guidance for the off-site search.”<sup>102</sup> In what appears to have been a strategic decision, counsel for Hill primarily focused his appeal on the seizure of the media, and only briefly discussed whether some sort of search protocol or guideline was required.<sup>103</sup> First, Hill argued that a plausible case can be made that computer searches are different than searches of physical documents, because computer forensic search tools allow for more narrowly tailored searches than are possible with paper documents.<sup>104</sup> With this as a premise, Hill claimed that the supporting affidavit for the search warrant should have explained why computer search tools could not have been used to narrow the search, thereby allowing the magistrate to make an informed decision as to the necessity of using such tools.<sup>105</sup>

The Ninth Circuit faulted Hill’s argument on two grounds. First, it agreed with and adopted the trial court’s analysis regarding Hill’s proposed search methodology.<sup>106</sup> At trial, Hill argued that the search “should have been limited to certain files more likely to be associated with child pornography, such as those with a ‘.jpg’ suffix . . . or those containing the word ‘sex’ or other key words.”<sup>107</sup> The Court recognized, correctly, the gross inadequacy of the proposed methodology, which could be thwarted by

---

<sup>101</sup> 452 F.3d 1140 (9th Cir. 2006).

<sup>102</sup> Appellant’s Reply Brief, *supra* note 16, at 4.

<sup>103</sup> *See id.*; Audio Recording of Appellate Oral Argument, *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006), [hereinafter Audio Recording of Appellate Oral Argument] (on file with author).

<sup>104</sup> Audio Recording of Appellate Oral Argument; Appellant’s Reply Brief, *supra* note 16, at 4-5.

<sup>105</sup> Appellant’s Reply Brief, *supra* note 16, at 4-5.

<sup>106</sup> *United States v. Hill*, 459 F.3d 966, 977-978 (9th Cir. 2006).

<sup>107</sup> *Id.* at 978.

changing file names or hiding data<sup>108</sup> (for example, by placing the files in an encrypted file or files).<sup>109</sup>

The Court's response, however, goes much further, stating that "[t]here is no way to know what is in a file without examining its contents."<sup>110</sup> In doing so, the Court perpetuates a myth founded on a technical error, which will be explored in depth in the following section. In addition, the Court explicitly rejected Hill's implicit assumption that a warrant supporting an affidavit *requires* either a search protocol or an explanation of its absence. While noting that it "look[s] favorably upon the inclusion of a search protocol," the court held that a search protocol was not necessary, in part because the actions of the officer conducting the search remain subject to judicial review.<sup>111</sup>

## 2. *Hill* and *Adjani*: Computer Search Rules in the Ninth Circuit

It is not clear why courts applying the Ninth Circuit's analysis in *Hill* would need to bother with judicial review. If the only way to know the contents of a file is to examine it, and no specific methodology or tool is required, then an officer would be justified in opening any file on any computer disk. The Court attempts to distance itself from this outcome:

even though a warrant authorizing a computer search might not contain a search protocol restricting the search . . . the officer is always 'limited by the longstanding principle that a duly issued warrant . . . may not be used to engage in a general, exploratory search.'<sup>112</sup>

But the Court declines to offer any guidance on precisely what the computer search version of the "longstanding rule" might look like. Similarly, the Ninth Circuit is careful to say that there are limits on what files the police can open while conducting a computer search.<sup>113</sup> They are just as careful, however, not to reveal what those limits are.<sup>114</sup> Instead, the Ninth Circuit refers to its own language in *United States v. Adjani*,<sup>115</sup> decided in the same term as *Hill*, and merely states that "[innocent and inculpat[ing]] computer files are often intermingled" but declines to define the proper

---

<sup>108</sup> *Id.* at 978-79.

<sup>109</sup> Encrypting a file (or multiple files into a combined file) causes its contents to appear to the computer as a series of random characters. CASEY, *supra* note 82, at 206. The encrypted file can be given any name. As a result, keyword searching encrypted files is ineffective.

<sup>110</sup> *Hill*, 459 F.3d at 978.

<sup>111</sup> *Id.*

<sup>112</sup> *Id.*

<sup>113</sup> *Id.*

<sup>114</sup> *Hill*, 459 F.3d at 978 n.14.

<sup>115</sup> *United States v. Adjani*, 452 F.3d 1140 (9th Cir. 2006).

steps for the police to take in conducting computer searches.<sup>116</sup> On this issue, the *Adjani* decision rests on the same technically flawed foundation as the *Hill* decision; the facts in *Adjani* help highlight an unwanted consequence of the Ninth Circuit's technical argument: the argument justifies opening any file on a suspect's computer.

As in *Hill*, the defendants in *Adjani* objected to the breadth of a computer search after inculpatory evidence was found on a defendant's computer.<sup>117</sup> The *Adjani* defendants were suspected of extortion; the police executed a search warrant that listed email and chat transcripts between certain individuals as items to be searched for and seized, and they discovered email sufficiently incriminating to support a charge of conspiracy to commit extortion.<sup>118</sup> Conspiracy was not one of the crimes listed in the warrant.<sup>119</sup>

First, the *Adjani* defendants argued that the warrant was overbroad because, although there was a detailed search protocol, it did not limit which emails or chat transcripts the police could look at (e.g., by email address or specific keywords).<sup>120</sup> In response, the Ninth Circuit noted that "such a pinpointed computer search, restricting the search to an email program or specific search terms, would likely have failed to cast a sufficiently wide net to capture the evidence sought."<sup>121</sup> As with *Hill*, the foundation of the argument was the defendant's ability to change file names: "The government should not be required to trust the suspect's self-labeling when executing a warrant."<sup>122</sup> Second, the defendants argued that the email in question was beyond the scope of the warrant because it implicated one of the defendants, who was not at that point charged with a crime, in conspiracy, which was not one of the crimes listed in the warrant.<sup>123</sup>

In an analogous non-digital search, the evidence would come in under the rule from *Horton v. California*,<sup>124</sup> which held that regardless of the searching officer's subjective intent, evidence of a separate crime found in plain view is admissible so long as the officer's search was objectively reasonable.<sup>125</sup> In *Horton*, a police officer who wanted a warrant for the fruits of a robbery and the weapons used to commit the robbery was only able to obtain a warrant for the former.<sup>126</sup> Despite the warrant's limitations, the officer searched the suspect's house with the intent of finding the weapons,

---

<sup>116</sup> *Hill*, 459 F.3d at 978 n.14.

<sup>117</sup> *Adjani*, 452 F.3d at 1142-43.

<sup>118</sup> *Id.* at 1149.

<sup>119</sup> *Id.* at 1151.

<sup>120</sup> *Id.* at 1149-50.

<sup>121</sup> *Id.*

<sup>122</sup> *Id.* at 1150.

<sup>123</sup> *Adjani*, 452 F.3d at 1151.

<sup>124</sup> *Horton* is also discussed in Part I.B, *supra*.

<sup>125</sup> *Horton*, 496 U.S. at 141-42.

<sup>126</sup> *Id.* at 131.

but confined his search to areas where the fruits of the robbery could be found.<sup>127</sup> The warrant justified intruding on the suspect's privacy to the degree necessary to find the fruits of the robbery, and so the Supreme Court saw no reason to require that the officer's discovery of the weapons be inadvertent.<sup>128</sup>

The essential requirement, then, is that the search must objectively appear to be confined to areas where the evidence sought can be found. Without citing *Horton*, the *Adjani* court refused to exclude the evidence, stating that "[t]here is no rule . . . that evidence [of a related crime] turned up while officers are rightfully searching in a location under a properly issued warrant must be excluded[.]"<sup>129</sup> Because the warrant allowed the police to search the defendant's computer for evidence of extortion, any evidence of a related crime found in plain view in an area where the police are entitled to search is admissible.<sup>130</sup>

The Ninth Circuit contrasted its holding in *Adjani* with *United States v. Carey*,<sup>131</sup> an influential Tenth Circuit case. In *Carey*, a police officer armed with a warrant to search for evidence of drug dealing opened a suspiciously named file and discovered evidence of child pornography.<sup>132</sup> Without obtaining a new warrant, the officer began to search for more evidence of child pornography.<sup>133</sup> The Tenth Circuit excluded all but the first image the officer found, holding that the officer's subjective intent to expand the scope of the search required a second warrant.<sup>134</sup> A number of commentators have argued that *Carey*'s focus on the officer's subjective intent is incompatible with the Supreme Court's rule in *Horton*.<sup>135</sup> In *Adjani*, the Ninth Circuit claimed they "need not decide" whether evidence of unrelated crimes is admissible.<sup>136</sup> Indeed they do not. Under *Horton*, such evidence is admissible, so long as the police were searching in a permissible location and manner.

Under *Hill* and *Adjani* the parameters of the computer search determine the scope of what evidence is admissible. *Hill* held that search protocols are not necessary.<sup>137</sup> *Adjani* held that evidence of *related* crimes is admissible if the evidence is in plain view during a search of a legitimate "location."<sup>138</sup> But, to comply with *Horton*, there can be no requirement that

---

<sup>127</sup> *Id.*

<sup>128</sup> *Id.* at 141.

<sup>129</sup> *United States v. Adjani*, 452 F.3d 1140, 1151 (9th Cir. 2006).

<sup>130</sup> *Id.*

<sup>131</sup> 172 F.3d 1268 (10th Cir. 1999).

<sup>132</sup> *Carey*, 172 F.3d at 1271-72.

<sup>133</sup> *Id.*

<sup>134</sup> *Id.* at 1273.

<sup>135</sup> *See, e.g., Ziff, supra* note 39, at 852-58.

<sup>136</sup> *United States v. Adjani*, 452 F.3d 1140, 1151 (9th Cir. 2006).

<sup>137</sup> *United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006).

<sup>138</sup> *Adjani*, 452 F.3d at 1151.

evidence of additional crimes be “related.” In both cases, the Ninth Circuit states that the police should not have to depend on file names, but rather must be able to examine files to determine their content.<sup>139</sup> If “examine” means “open,” then a *Horton*-compliant version of the Ninth Circuit’s rules allow police armed with a warrant for one crime to open any file on a suspect’s hard drive or storage media, and any evidence found, of any crime, would be admissible. This is the epitome of a general search.

Search protocols narrow the scope of a search by defining both the object of the search (e.g., child pornography) and the search methodology (e.g., keyword searching, opening all picture files, etc.).<sup>140</sup> However, there is no textual support for search protocols in the Fourth Amendment, and, as a general rule the police are not required to explain beforehand how they are going to conduct a search.<sup>141</sup> Thus, arguing that search protocols are required begs the question of whether searching an entire hard drive violates the Fourth Amendment. Assuming *Horton* is not overruled, the key to a rule that both allows police to find relevant evidence and still prevents them from searching suspects’ entire hard drives for evidence of any crime is a better understanding of what type of “examination” police must do to determine whether a computer file—or even a remnant of a file—contains evidence.

### 3. Two Approaches to Computer Searches

The Supreme Court has established that law enforcement officers are not required to use the least intrusive technique available when conducting a search.<sup>142</sup> Some courts have relied on this rule to hold that the Fourth Amendment does not require the use of search protocols or forensic software to limit police intrusion into innocent computer files.<sup>143</sup> One commentator specializing in Fourth Amendment issues, Thomas Clancy, has argued that any other result is an unjustified “special approach” based on the mistaken belief that the computers are “so fundamentally different from anything in the past” as to make traditional Fourth Amendment rules inapplicable.<sup>144</sup> In Clancy’s view, computers are “container[s] of a variety of items, ranging from wires to hard drives, some of which hold (contain!) digital

---

<sup>139</sup> *Id.*; *Hill*, 459 F.3d at 977-78.

<sup>140</sup> *See, e.g.*, *United States v. Brooks*, 427 F.3d 1246, 1251-52 (10th Cir. 2005).

<sup>141</sup> *See Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 651-52 (1995) (stating that for search methods other than those existent at the time of the Fourth Amendment’s adoption, the appropriate test is “reasonableness”).

<sup>142</sup> *See, e.g., id.* at 663 (citing to collected cases).

<sup>143</sup> *See, e.g., United States v. Gray*, 78 F. Supp. 2d 524, 529 n.8 (E.D. Va. 1999).

<sup>144</sup> Clancy, *supra* note 51, at 204-06.

evidence.”<sup>145</sup> Clancy sees arguments based on the intermingled nature of documents on a computer as technical, rather than legal.<sup>146</sup>

Yet, Fourth Amendment jurisprudence is an adaptation of the sparse language of the amendment to the real world interplay between police and citizens. The rules regarding searches of containers arose not from a purely legal, Platonic ideal of the Fourth Amendment, but are based on practical, factual considerations of the nature of the things to be searched. In other words, the “technical” aspects of computer storage are as relevant in formulating sound Fourth Amendment rules as the practical considerations that gave rise to the traditional rules governing container searches. Knowing how evidence is “contained” on computers, and what kind of searches can discover evidence is essential to understanding whether the technical distinctions between computers and other containers should result in legal distinctions in Fourth Amendment search and seizure rules.

a. *What Gets Searched: A Brief Overview of Computer Storage*<sup>147</sup>

When the police “search a computer,” only the components that are capable of storing data are actually searched. The primary internal data storage location, and thus the primary source of evidence, in most computers is the hard drive.<sup>148</sup> Additionally, data may be stored on external sources (e.g., removable media), such as floppy disks, ZIP disks, CDs, DVDs, and removable flash memory-based devices (sometimes referred to as jump drives or thumb drives).

Regardless of the type of media, computer data is simply a collection of ones and zeros<sup>149</sup> organized into groups. Both the physical device (e.g., the hard drive) and the software operating system (e.g., Windows XP) utilize the smallest useable group size for storage purposes. For example, the smallest useable group of ones and zeros on a hard drive is frequently called a *sector*, and may be composed of 512 bytes worth of data—enough to hold 512 characters.<sup>150</sup> The smallest group at the software level is often

---

<sup>145</sup> *Id.* at 216.

<sup>146</sup> *Id.* at 210.

<sup>147</sup> For the sake of simplicity, this note uses “operating system” generically to refer to both the operating system and the file system. For the practical purposes of this note, the distinction is not critical.

<sup>148</sup> CASEY, *supra* note 82, at 200. Data can also be retrieved from the Random Access Memory, BIOS, and potentially from other devices using flash memory. While police and experts often avail themselves of those resources, they are not essential for this discussion.

<sup>149</sup> For example, on a hard drive, a positive magnetic charge might represent a one, and a negative charge might represent a zero; on a CD-R, a pit in the surface might be a one, and the absence of a pit (i.e., a smooth surface), might be a zero.

<sup>150</sup> CASEY, *supra* note 82, at 198-201.

called a *cluster*.<sup>151</sup> The number of sectors that make up a cluster varies by operating system and storage media size. For example, a computer running Windows<sup>152</sup> might have clusters made up of 64 sectors (roughly 32 kilobytes).<sup>153</sup> Once part of a cluster is used, the operating system (e.g., Windows) marks the entire cluster as used.<sup>154</sup> For example, if a user wants to save a 100 kilobyte file in the Windows system just described, the file will span four clusters. The first three will be completely filled, but only the first four kilobytes of the last cluster will be used. The operating system, however, will consider all four clusters to be unavailable for the purposes of storing additional data.

Finally, because files can span multiple clusters, the operating system must also do some additional work. It must track which clusters are being used to store data, which clusters are available to store data (i.e., which clusters are “empty”), the location and relationship of clusters being used to store data (e.g., for the 100 kilobyte file above, which cluster contains the first part of the file, which contains the second, etc. and where each cluster is located), and the file name and folder name associated with each file.<sup>155</sup>

b. *The Simple Method: Manual Searching within the Operating System*

The simplest search approach is to turn on the suspect’s computer and simply start looking around for incriminating files, starting, for example, in the My Documents folder, and then browsing through the various folders until the officer sees something that catches his or her eye.

There are many drawbacks to this method. First, it is inefficient: most computers contain hundreds of thousands of files.<sup>156</sup> Additionally, the suspect may have attempted to hide incriminating evidence. If the suspect simply changed the file name or extension, the police officer could simply open the file to see what it contained; but to be certain he had not been fooled, the officer would have to open every file on the computer. Even if he did so, vast amounts of evidence could remain undetected. For example, deleted files would remain undetected, as would information only temporarily stored on a hard drive, but still available in part of a cluster.<sup>157</sup> A sophisticated criminal might make the disk appear smaller than it actually is,<sup>158</sup> and store evidence in a hidden partition, or hide a file containing evidence in

---

<sup>151</sup> *Id.* at 200.

<sup>152</sup> Using Windows’ FAT file system.

<sup>153</sup> CASEY, *supra* note 82, at 203.

<sup>154</sup> *Id.* at 208.

<sup>155</sup> *Id.* at 202-05.

<sup>156</sup> For example, the computer this Note is being typed on has over 525,000 files on it.

<sup>157</sup> See CASEY, *supra* note 82, at 208-09.

<sup>158</sup> For example, the user could edit the maintenance track of the hard drive. See *id.* at 201.

another file (for example, in an encrypted file, or, using a technique called steganography, in a picture file).<sup>159</sup>

Second, this type of search creates evidentiary problems: every time storage media is accessed in read/write mode, and particularly when the hard drive is being searched in the method described above, data can be written to the storage media. While some obvious sources of evidence such as Word documents and picture files aren't going to be damaged, some less obvious sources of evidence will be.<sup>160</sup> The operating systems and the drive contain data *about* the evidence files, such as the last access time, and time of creation, that may prove important when attempting to demonstrate the knowledge or intent of the suspect. This information may be overwritten by opening files, or simply turning on the computer.<sup>161</sup> Each change also defeats a common authentication technique, called *hashing*, that police and forensic experts use to prove that evidence is authentic and has not been subjected to tampering.<sup>162</sup>

Finally, a simple search may result in a loss of evidence. When a file is deleted, the clusters containing the data for that file are simply marked as available for later use.<sup>163</sup> Until the clusters are actually overwritten with new data, the data can be recovered using special tools.<sup>164</sup> Simply using the operating system creates the risk that clusters containing evidence in the form of deleted or temporary files may be overwritten.<sup>165</sup>

In short, the drawbacks to this method are so severe that investigative groups specializing in computer crimes and investigations have developed guidelines and procedures to ensure that it is not used. Instead, they apply a combination of procedures and specialized tools, known collectively as computer forensics, to conduct their investigations.<sup>166</sup>

---

<sup>159</sup> See, e.g., Ewa Huebner, Derek Bem et al., *Data Hiding in the NTFS File System*, 3 DIGITAL INVESTIGATION 211 (2006) (discussing data hiding techniques).

<sup>160</sup> CASEY, *supra* note 82, at 224.

<sup>161</sup> *Id.* at 311-15.

<sup>162</sup> Hashing is the process of running a mathematical algorithm against a file or group of files (including an entire hard drive) to derive a unique combination of letters and numbers, called the *hash*. If so much as one bit changes in the file set, the hash value will differ. Thus, if an expert hashes a hard drive at the time of acquisition it can be hashed later to prove that nothing has been altered (or added). Hashing can also be used to prove that a copy of a drive or file is complete and accurate. See CASEY, *supra* note 82, at 218-20 (discussing the MD5 hashing process).

<sup>163</sup> *Id.* at 203-05.

<sup>164</sup> *Id.* at 264-66.

<sup>165</sup> For example, the Windows operating system creates a "page file" on the hard drive, which it uses to temporarily store information, much as it does with RAM.

<sup>166</sup> See, e.g., *id.* at 627-644; UNITED STATES DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), <http://www.cybercrime.gov/s&smanual2002.htm>.

c. *The More Effective Method: Computer Forensics*

The physical world equivalent of the simple search described in the previous section might be an officer walking into a murder scene with muddy boots, removing, bare-handed, a knife from the victim, dropping it in his coat pocket and returning to the office. One would expect, instead, for the scene to be carefully photographed, blood evidence to be collected for sampling, the murder weapon and other physical evidence carefully bagged, labeled and removed, with the chain of possession documented throughout the investigation.

A forensic search of computer is closer to the second method, although with some unique advantages.<sup>167</sup> Imagine if the police could clone the entire crime scene and cart it off to storage while they performed their work on the copy. That is exactly what happens in a computer forensic investigation. Instead of working on the original drive or storage media, a forensic investigator typically creates a bitstream copy.<sup>168</sup> By doing so, the forensic investigator captures not only the files that can be seen when the user is booted into the operating system, but deleted files and empty space as well.<sup>169</sup> Both drives can be hashed, and the values compared to verify that a complete and accurate copy was made.<sup>170</sup>

Next, the forensic investigator will usually attach the drive in read-only mode<sup>171</sup> to a computer equipped with computer forensic examination software, such as Guidance Software's EnCase.<sup>172</sup> Attaching the copy of the suspect's drive to another computer bypasses the operating system installed on the suspect's hard drive, so that every file, including the operating system files, appears as an ordinary file, capable of being searched and opened.<sup>173</sup> Forensic software significantly extends forensic investigators' ability to search for evidence. Instead of being limited to searching for and opening active files (i.e., files that have not been deleted), investigators using forensic software can search the contents of every sector and cluster of the hard drive; they can also look at *parts* of files without "opening"

---

<sup>167</sup> For starters, a lack of blood.

<sup>168</sup> CASEY, *supra* note 82, at 108-109, 225-228.

<sup>169</sup> *Id.*

<sup>170</sup> *Id.* at 218-220.

<sup>171</sup> In read-only mode, a computer can read from storage media, but cannot write to it. Some media, such as CDs and DVDs (including CD-Rs and DVD-Rs that have been finalized), are always read-only. Other media, such as hard drives or floppy disks, can be mounted (attached to the computer and recognized by the operating system) in either read-only or read/write mode.

<sup>172</sup> EnCase is the most widely used commercial forensic software product. Other options include Access Data's Forensic Toolkit (FTK), and specialized distributions of the Linux operating system, such as e-Fense's Helix (<http://www.e-fense.com/helix/>). While this Note uses EnCase in its examples, other forensic software products offer similar features.

<sup>173</sup> Assuming the forensic workstation's operating system is capable of identifying the file system on the attached drive.

them in the normal sense of the word.<sup>174</sup> When a file is deleted, the clusters used to store the file are simply marked as available to be used for storing new data. The operating system hides those clusters from the user, and, when space is needed, overwrites the clusters. Until the clusters containing a file are overwritten, however, the data from the file is still present, and can be recovered using forensic software. Even if a file cannot be recovered, one or more of the clusters that made up the file may still contain data from the original file.<sup>175</sup>

Forensic tools like EnCase not only increase the amount of data investigators can access, they also significantly enhance the ability to search for and find evidence. For example, investigators can reduce the number of files to be searched by eliminating common operating system and program files,<sup>176</sup> automatically recovering many deleted files, searching either the entire hard drive or active files for specified keywords or phrases, identifying and previewing image files, and identifying and flagging encrypted files. Notably, EnCase includes a script that quickly identifies mismatched file extensions.<sup>177</sup> Investigators using the program<sup>178</sup> can thus easily detect when a suspect has changed a file extension in an attempt to hide evidence. In *Hill*, the police used EnCase,<sup>179</sup> and it is nearly certain that either the same or similar software was used in *Adjani*—experts searched the defendant’s computers at the FBI Computer Laboratory.<sup>180</sup>

It would seem that the possibility of users changing file extensions, then, is more likely to fool judges than police officers. As a justification for opening any and every file on a suspect’s storage media, the argument is technically flawed. Even if one views the changed file extension argument as a proxy for the proposition that all files must be subject to being opened to know their contents—an approach that treats files as containers—the end result is untenable: law enforcement officers can dissect a suspect’s hard

---

<sup>174</sup> KRUSE & HEISER, *supra* note 83, at 170-74.

<sup>175</sup> This is true even if part of the cluster has been overwritten. For example, consider a 100 Kilo-byte file spanned over four clusters. Suppose that the file was deleted, and then the first cluster, which was completely full, was later used to store the last two kilobytes of another file. The file system would treat the entire cluster as used by the new file, but all but the first two kilobytes would contain data from the old file.

<sup>176</sup> See CASEY, *supra* note 82, at 638-39. For example, the police can hash all of the files on the suspect’s drive and then compare the values against a library of known hash values for common program files. If the hashes match, the police can rule the file out as a source of evidence. A similar method can be used to detect known non-innocent files. For example, the FBI maintains a hash library of known child pornography. A “hit” quickly tells police that there is child pornography on the suspect’s computer.

<sup>177</sup> Guidance Software, EnCase Forensic Detailed Product Description 4 (2006), available at [http://www.guidancesoftware.com/products/ef\\_index.asp](http://www.guidancesoftware.com/products/ef_index.asp) (click on “Detailed Product Description (PDF)”).

<sup>178</sup> Or similar software, such as AccessData’s Forensic Tool Kit (FTK).

<sup>179</sup> See *Hill Trial*, 322 F. Supp. 2d 1081, 1092 (C.D. Cal. 2005).

<sup>180</sup> *United States v. Adjani*, 452 F.3d 1140, 1144 (9th Cir. 2006).

drive looking for evidence of any crime, and there is no room for meaningful judicial review.

#### 4. Problems with the Ninth Circuit's Computer Search Rules

If Clancy's view of computers as containers<sup>181</sup> was correct, *Hill* would justify allowing law enforcement officers to search every file for evidence, and, under *Adjani*, almost any evidence found—of any crime—would be admissible. In one sense, Clancy *is* correct. Computers certainly can contain evidence. The police, however, are not interested in what is physically “contained” in computer storage media. They are not interested in magnetic charges or pits on an optical surface that represent ones and zeros—they are interested in the data that those ones and zeros represent.

From the preceding sections, however, it is clear that what the digital evidence police are interested in is not only physically contained on hard drives, but virtually contained as well. Making matters more complicated, what constitutes a container depends on the search method used. If the police perform a simple search from within the operating system, they will only be able to see files, making files the relevant “containers.” If, however, the police use forensic tools, the “containers” become the sectors and clusters (which may or may not make up a complete file) on the storage media. Applying container rules to a physical container that contains virtual digital containers that transmogrify when viewed with different software tools is more likely to result in a philosophical quagmire than a clear legal rule.

The Ninth Circuit stated that “[t]here is no way to know what is in a file without examining its contents.”<sup>182</sup> If the police are conducting a simple search from within the operating system, then “examine” means “open,” but the “containers” that can be opened are limited to files. This is an unsatisfactory result, because evidence described in a warrant could be contained in a previously used cluster that has been marked as available. For example, if the warrant allows the police to search for evidence of a ransom attempt, a crucial piece of evidence might be the phrase “bring \$1,000,00 to the old tree.” Even if the file containing the phrase were deleted, the phrase might still be on the computer, tucked away in a cluster marked as available.<sup>183</sup> Thus, while the police would be allowed to open every container (i.e., file), they would not be able to find evidence clearly covered by the warrant.

---

<sup>181</sup> See Clancy, *supra* note 51, at 195.

<sup>182</sup> *United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006).

<sup>183</sup> In some operating systems, the phrase might even be recoverable after the cluster was recycled. For example, if the phrase were contained at the end of the cluster, and only the first few bytes of the cluster were used for a new file, the phrase would not be overwritten and might be discovered through keyword searching. See CASEY, *supra* note 82, at 205.

On the other hand, if the police are conducting a forensic search, “examine” could involve scanning, keyword searching, hashing, or any number of automated functions that do not involve actually opening files, and the “containers” would be sectors or clusters. Thus, while the police may need to “examine” every file (and perhaps every sector), they would not actually need to *open* every file. Indeed, in the ransom note example, opening every file would not yield the evidence, regardless of what the name of the file was. Yet, even though the rationale for allowing the police to open every file is gone, if sectors or clusters are the containers, traditional container rules allow every part of the hard drive to be searched.

Applying physical container rules to virtual, digital containers leads to inconsistent results. Hill suggested that at least one forensic search technique (keyword searching) should have been used to limit the search, and the Ninth Circuit responded by stating that police must be able examine every file to determine its contents.<sup>184</sup> In this case, “examine” meant “open,” since a keyword search across every file, though an examination in some sense, is precisely what the court found to be inadequate.<sup>185</sup> Essentially, the Ninth Circuit responded to a forensic search container argument with a simple search container answer. But, as previously noted, the rules are different. If every file must be opened to know its contents, then the search must be the simple variety, in which case large amounts of potentially relevant data is not available. A forensic search allows the police to search all of the data on the drive, but makes it unnecessary to open all files.

Whether the police are *allowed* to open every file or sector on a hard drive during a search is a different question. While the police are not required to use the least intrusive means necessary to perform a search, the relative degree of intrusiveness is relevant in determining whether a search is reasonable.<sup>186</sup> Indeed, cases that state the rule often also explain why the proposed, less intrusive means were unworkable.<sup>187</sup> Computer searches raise difficult questions. Which is more intrusive: a simple search that leaves much of the hard drive unexplored but justifies randomly opening files, or a forensic search that allows every part of the drive to be searched but also allows the use of tools to exclude non-relevant data?

By hypothesis, in a simple search nearly every file is equally capable of containing evidence<sup>188</sup> and the only way to know what a file contains is to open it. If forensic tools are available, they should be required, not be-

---

<sup>184</sup> *Hill*, 459 F.3d at 977-78.

<sup>185</sup> *Id.*

<sup>186</sup> *See Skinner v. Ry Labor Executives Ass’n*, 489 U.S. 602, 629 n.9 (1989).

<sup>187</sup> *E.g., id.* at 631; *Vernonia Sch. Dist. 47J v Acton*, 515 U.S. 646, 663-64 (1995).

<sup>188</sup> In some cases, some files could be excluded. For example, if the police were searching for a movie file, there would be no reason to open files that were only a few kilobytes in size, regardless of the file names.

cause they are the least intrusive means of conducting the search, but because their existence and availability makes the alternative method unreasonable. A hit-or-miss approach to searching that fails to protect individual privacy interests can hardly be reasonable when tools are available that are far, far more likely to achieve the social goal of catching guilty criminals, while, as a side benefit, providing tools that can minimize privacy invasions. Yet, once the forensic tools are used, the rules shift. Now every sector is available for searching, and although the search *can* be narrowly tailored, it doesn't have to be. Broad and narrow forensic searches offer the same social benefit. When the benefit is the same, the Supreme Court does not require that the least intrusive means be used.<sup>189</sup>

This can hardly be the outcome the Ninth Circuit had in mind in *Hill*. The court stated that there were limits to what police could do during a computer search.<sup>190</sup> The Ninth Circuit's explanation for why the defendant's search methodology was unacceptable, however, pushes the court down a contorted path of reasoning in which computer files are stored in fluctuating virtual containers, each with their own rules. Little room is left for comprehensible limitations on computer searches.

The Ninth Circuit's recent decision in *United States v. Comprehensive Drug Testing, Inc.*<sup>191</sup> highlights just how contorted that path is. In *Comprehensive Drug Testing* ("CDT"), federal agents obtained warrants to search two drug testing laboratories and seize drug testing information and specimens related to ten Major League Baseball players, and ancillary documentary and explanatory materials.<sup>192</sup> During their search, agents discovered a "master list" of the names and identifying numbers of all baseball players tested.<sup>193</sup> Among the items seized, the agents copied a computer directory containing "all of the computer files for CDT's sports testing programs."<sup>194</sup> Based on the information contained in the directory, investigators learned of over 100 additional players who had tested positive for steroids, and obtained a second warrant for additional information.<sup>195</sup> In response, the defendants filed Fed. R. Crim. P. 41(g) motions requesting that all evidence not related to the ten players named in the original warrant be returned.<sup>196</sup> The motions were granted, and the government appealed.<sup>197</sup>

---

<sup>189</sup> See *Skinner*, 489 U.S. at 631; *Vernonia*, 515 U.S. at 663-64.

<sup>190</sup> *Hill*, 459 F.3d at 978.

<sup>191</sup> *United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915 (9th Cir. 2006). The government was seeking the information in connection to its investigation of Balco, a company that allegedly provided steroids to Major League Baseball players. *Id.* at 919-20.

<sup>192</sup> *Id.* at 921.

<sup>193</sup> *Id.* at 923.

<sup>194</sup> *Id.* at 922.

<sup>195</sup> *Id.* at 923-24.

<sup>196</sup> *Comprehensive Drug Testing*, 473 F.3d at 924.

<sup>197</sup> *Id.*

The Ninth Circuit held that the seizure of the computer directories containing the information that led to the second warrant was reasonable.<sup>198</sup> In doing so, it pointed out that the seizing agents thoughtfully copied the directories, rather than take the entire computer or perform a highly inconvenient on-site search.<sup>199</sup> Because the government still needed the information in the directory to conduct its investigation, the Ninth Circuit found that granting the motions to return the evidence was “unjustified and improper.”<sup>200</sup> Under *Hill* and *Adjani*, decided just months earlier, that should have been the end of the inquiry. The agents lawfully seized computer data that could contain evidence—they should have been able to search it in its entirety.

Instead, the Ninth Circuit held that, “while the government may seize intermingled data for off-site review to minimize intrusiveness of a computer search, it may not retain or use the evidence after proper objections are raised, unless a magistrate subsequently reviews and filters the evidence off-site.”<sup>201</sup> It is difficult to overstate how fundamentally confused this approach is. Consider the Ninth Circuit’s rules in sum: (1) after explaining to a neutral magistrate the unchanging facts that support doing so, the police may seize all computer media (even media that cannot reasonably be believed to contain evidence); (2) the police may “examine” every file (and “examine” seems to mean “open”); and (3) a search protocol is not required by the Fourth Amendment; but, (4) the Fourth Amendment requires that, upon objection, a neutral magistrate must review and filter the evidence.

Apart from its incoherence, there are two practical flaws to this approach. First, it fails to protect privacy interests, which is the primary point of the Fourth Amendment. A search protocol protects privacy interests by ensuring that only relevant information is seen. The review by the magistrate, however, happens either after or contemporaneously with viewing *all* of the information, in order to separate the relevant from the non-relevant. Secondly, it requires magistrates to perform a role for which they are ill suited. Remember that the evidence being reviewed and filtered is massive amounts of computer data. Either the magistrate must be able to perform his or her own forensic examination, or he must sort through the sub-set of information provided by the government. The latter option defeats the purpose of rule.

---

<sup>198</sup> *Id.* at 938.

<sup>199</sup> *Id.* at 932.

<sup>200</sup> *Id.* at 937-38.

<sup>201</sup> *Id.* at 940.

## III. A PROPOSAL FOR A BETTER RULE

The first step for the Ninth Circuit, and courts in general, is to stop justifying specific instances of law enforcement officers opening *a* file with the argument that they must be able to open *any* file to know what it is, and abandon the container analogy that supports the argument. As Raphael Winick first argued in 1994, treating hard drives as containers fails to recognize key differences between the digital and physical world.<sup>202</sup> And, as this Note has argued, one of those differences is that the only relevant candidates for “containers” are files or the clusters and sectors that comprise them, not the physical storage media itself. Applying traditional container rules to virtual containers only highlights how poorly those rules fit.

Winick believed that the Ninth Circuit should treat hard drives like file cabinets containing vast amounts of intermingled documents, and apply its rule from *Tamura*; wholesale seizures should be authorized in advance by an informed neutral magistrate.<sup>203</sup> In essence, the Ninth Circuit followed his advice in announcing the new rule discussed in Part II.A. As that Part makes clear, the new rule fails to recognize the practical realities of computer searches. File cabinets are physical things holding static physical documents. Computer storage media are physical things holding dynamic digital data that, as a general rule, requires off-site searching. While better than the container analogy, the file cabinet analogy is still inappropriate.

In cases where a magistrate approves a wholesale seizure, Winick argued that “[t]he basic principle is that before a wide-ranging exploratory search is conducted, the magistrate should require the investigators to provide an outline of the methods that they will use to sort through the information.”<sup>204</sup> The police should be required to use scope-narrowing techniques such as keyword searching and the parties should bargain for, and the magistrate approve, the least intrusive search method—another way to describe a search protocol.<sup>205</sup> In *Hill*, however, the Ninth Circuit refused to require the use of search protocols, stating that they “looked favorably” upon them, but that failure to use one was “not fatal.”<sup>206</sup>

On this point, the Ninth Circuit was correct. In many cases, search protocols are sensible. They provide the defendant an opportunity to convince the court and/or the police to use a minimally intrusive search method, they offer assurance to the police that if they follow the approved methods their search is unlikely to be overturned, and they aid courts in making efficient decisions about later objections. It is not clear, however,

---

<sup>202</sup> Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 109-11 (1994).

<sup>203</sup> *Id.*

<sup>204</sup> *Id.* at 108.

<sup>205</sup> *Id.*

<sup>206</sup> *United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006).

that they are constitutionally mandated, and there are situations in which a search protocol may not be helpful. For example, if a criminal is particularly sophisticated, the police may find that their initial search yields only enough evidence to know that a different search protocol is required, a process which could be repeated multiple times. The highly technical nature of computer searches may lead courts to use protocols from cases that were challenged on appeal and survived as generic templates for protocols in other cases, leading to rigid structures that unreasonably prevent police from adapting to changes in criminal methodology.

A better solution is to focus on judicial review of police searches, applying general Fourth Amendment principles to computer searches, rather than complicated jurisprudential rules designed to fit roughly analogous physical world conditions. Courts should use the following guiding principles: (1) the primary requirement of Fourth Amendment searches is that they must be reasonable;<sup>207</sup> (2) determining “reasonableness” requires assessing the totality of the circumstances, and balancing the suspect’s privacy interests against the government’s interest in promoting its legitimate goals;<sup>208</sup> (3) searches carried out pursuant to a warrant are presumed reasonable; (4) the least intrusive search is not required; and (5) the officer’s objective behavior is relevant to determining reasonableness, but subjective intent is not.<sup>209</sup>

The third principle has a powerful impact. If a law enforcement officer establishes that there is sufficient probable cause to search a computer for evidence of a specific crime and obtains a search warrant, his search is presumptively reasonable. A rule governing judicial review of computer searches cannot, as Winick suggests, simply “ensure that the officers only read through files that there is reason to believe contain relevant information,”<sup>210</sup> a requirement that could severely limit officers’ ability to find evidence by requiring them to justify why they opened each and every questioned file. Such a rule destroys the presumption of reasonableness, and also violates the principle that the least intrusive means is not required. Instead, the rule must be crafted to identify only significantly unreasonable behavior while leaving law enforcement officers sufficient room to “cast a sufficiently wide net to capture the evidence sought.”<sup>211</sup>

Turning to the second principle, “reasonableness” requires balancing the suspect’s privacy interests against the government’s interest, in the totality of the circumstances. In the case of computer searches, the government’s interest is in finding the evidence described in the warrant. A computer search is unreasonable, then, when the invasion of the individual’s

---

<sup>207</sup> *Hill Trial*, 322 F. Supp. 2d 1081, 1088 (C.D. Cal. 2005).

<sup>208</sup> *United States v. Knights*, 534 U.S. 112, 118-19 (2001).

<sup>209</sup> *Horton v. California*, 496 U.S. 128, 138-39 (1990).

<sup>210</sup> Winick, *supra* note 202, at 108.

<sup>211</sup> *Hill*, 459 F.3d at 978 (quoting *United States v. Adjani*, 452 F.3d 1140, 1149 (9th Cir. 2006)).

privacy is not justified by the government's interest in finding the evidence described in the warrant. Because of the presumption that a search conducted pursuant to a warrant is reasonable, nearly any search designed to find the evidence described in the warrant overpowers the suspect's right to privacy.

After adding the fifth principle (that only the officer's objective behavior is relevant) the rule can be phrased as follows:

A computer search conducted pursuant to a warrant is unreasonable only if the officer's actions are such that a reasonable person could not conclude that the search was calculated to find the evidence described in the warrant.

This rule respects the presumption of reasonableness attendant with a warrant, does not require law enforcement officers to use the least intrusive search possible, protects individual privacy, and utilizes an objective test.<sup>212</sup> This is the test the Ninth Circuit should have adopted in *Hill*.

In many cases, applying the rule above would not have led to a different result. In part, this can be attributed to the nature of computer forensic searches, the complexity and ultimate purpose of which makes a reasonable search strategy almost necessary, and in part it can be attributed to the fact that in many of the cases, the defendants are clearly guilty. There is no doubt, for example, that Mr. Hill possessed child pornography. There is no doubt that the *Adjani* defendants were attempting to commit extortion. There is no doubt that, whatever their motive for doing so, the *CDT* laboratories actually possessed evidence of a crime described in a warrant. In all three cases, there are no legitimate indications that the police went on a fishing expedition for evidence of unrelated crimes.<sup>213</sup> It would be unfortunate indeed if the rule this Note proposes led to different outcomes in those cases.

The advantage of the proposed rule is not how it handles the majority of cases, it's how it handles the exceptional ones. To illustrate, consider the following scenario. The police obtain a warrant to seize a high-tech

---

<sup>212</sup> For example, consider the following the scenario. A police officer obtains a warrant to search for evidence of tax evasion and lawfully seizes the suspect's computer. At the lab, he hashes the files on the suspect's drive and compares them against the FBI's child pornography hash library. He gets 5 hits. Under *Hill's* technical argument, the evidence would be admissible, because the police could theoretically open any file on the hard drive (although the *Hill* court does imply that there are unspecified limits). Under the proposed rule, the evidence would not be admissible, because no reasonable person could conclude that it was calculated to find evidence of tax fraud.

<sup>213</sup> In *CDT*, the defense clearly believed that the government abused its warrant power, resulting in the discovery of the names of over one hundred additional athletes who were not named in the warrant, and who had tested positive for steroids. However, the discovery was made *after* the laboratories in question declined to produce the information of their own volition, which might have avoided the disclosure of the additional names. *United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915, 915-23 (9th Cir. 2006).

bookie's computer and all of his storage media to search for evidence of illegal online gambling and bookmaking. Being truly high-tech, the bookie has a large collection of old computers and old computer storage media. The officer executing the warrant seizes all of it and carts it away to the lab. At the lab, the forensic investigator makes a forensic copy of the suspect's primary computer and hashes the files on the drive. The investigator spent the morning examining the mayor's computer, which had been hacked, and, the mayor believes, had a highly embarrassing letter from an office intern copied from it.<sup>214</sup> On a lark, the investigator compares the hash of the letter with those of the suspect's drive and gets a hit. The letter is sitting in a folder entitled "business developments"—along with a number of documents related to bookmaking.

Assuming the warrant contained the appropriate boilerplate, a court applying *Hill* would be hard pressed to object to any aspect of the search. The boilerplate would not protect the accused from having his potentially valuable collection of old computers removed, regardless of how unlikely it is that they would contain evidence. If the court strictly applied the logic of *Hill*, the purloined file would have to be admitted, either because it was in a "place" the police were allowed to be,<sup>215</sup> or because the police would have to open each file to know its contents. If the court adhered to the spirit of the Ninth Circuit's vague statement that there are some unspecified limits to computer searches, the most likely result would be an incoherent ad hoc rule.

With the proposed rule, however, the result is clear and no adjustment is needed. No reasonable person could say that a hash search for the mayor's stolen letter was reasonably calculated to find the evidence of bookmaking described in the warrant. Moreover, the new rule protects the bookie's interest in the computers and storage media that could not reasonably be believed to contain the evidence.

Of course, not every instance of an unreasonable search that exceeds the scope of a warrant will be as clear as the preceding example. It is possible that a clever police officer may be able to expand his search beyond the warrant and cover up his behavior with a story designed to make the search seem reasonable. However, the more egregious the behavior, the less plausible the story will seem, and, unlike the *Carey* test, this Note's proposed test does not require the court to determine what the officer subjectively intended to do. Nor does it handcuff the officer with an inflexible search protocol, nor give him free reign to open any file on the suspect's computer under a misguided analogy to physical containers. What it does is provide some clarity for the rules governing computer searches and seizures.

---

<sup>214</sup> He's just waiting for the blackmail note. I thought we'd move away from child pornography.

<sup>215</sup> Using a pure version of the container analogy would yield the same result. Whether within files, folders, clusters or sectors, they could potentially "contain" the evidence sought.

## CONCLUSION

Fourth Amendment jurisprudence governing the searches of containers and intermingled physical documents arose out of factual considerations of the nature of the things to be searched. Examining the technical aspects of how computers store information and how computer searches can yield evidence exposes critical differences between computers and physical-world sources of evidence such as containers and file cabinets.

Formulating sound Fourth Amendment rules for computer searches requires recognizing those differences. The Ninth Circuit's decision in *United States v. Hill* illustrates the confusion that results from failing to do so. By relying on analogical arguments while trying to protect privacy interests, the Ninth Circuit inadvertently has created incoherent and unworkable rules for computer searches and seizures that burden magistrates and law enforcement officers, while failing to protect privacy interests.

By abandoning physical-world analogies and applying existing Fourth Amendment principles, courts can derive better rules for computer searches and seizures: (1) law enforcement officers should be able to seize all computer media that could reasonably be believed to contain the evidence described in a warrant without explaining why an on-site search is impractical; and (2) a computer search conducted pursuant to a warrant is unreasonable only if the officer's actions are such that a reasonable person could not conclude that the search was calculated to find the evidence described in the warrant.