

# Journal of Criminal Law and Criminology

---

Volume 100  
Issue 4 *Fall*

Article 6


---

Fall 2010

## Swinging for the Fences: How Comprehensive Drug Testing, Inc. Missed the Ball on Digital Searches

Vincent Angermeier

Follow this and additional works at: <https://scholarlycommons.law.northwestern.edu/jclc>

 Part of the [Criminal Law Commons](#), [Criminology Commons](#), and the [Criminology and Criminal Justice Commons](#)

---

### Recommended Citation

Vincent Angermeier, *Swinging for the Fences: How Comprehensive Drug Testing, Inc. Missed the Ball on Digital Searches*, 100 *J. Crim. L. & Criminology* 1587 (2010)

This Comment is brought to you for free and open access by Northwestern University School of Law Scholarly Commons. It has been accepted for inclusion in *Journal of Criminal Law and Criminology* by an authorized editor of Northwestern University School of Law Scholarly Commons.

## COMMENTS

### **SWINGING FOR THE FENCES: HOW COMPREHENSIVE DRUG TESTING, INC. MISSED THE BALL ON DIGITAL SEARCHES**

Vincent Angermeier\*

*This Comment offers a critical analysis of the recent decision of the Ninth Circuit Court of Appeals in United States v. Comprehensive Drug Testing, Inc. First, the Comment discusses the facts of the case and the decisions leading up to the en banc decision. The Comment goes on to review the evolution and purposes of the plain view doctrine. The Comment then argues that the Ninth Circuit's decision in Comprehensive Drug Testing, Inc. represents an overreaction to the privacy concerns raised by the application of the plain view doctrine to digital searches. Finally, it will advocate that courts continue to apply the plain view doctrine to digital searches, subject to heightened scrutiny by judges, who should grant warrants only when it is reasonable to do so in light of the strength of the probable cause, the severity of the crime being investigated, and voluntary actions taken by the government to reduce the social cost of the privacy intrusion.*

#### I. INTRODUCTION

As digital technology has become ubiquitous and inexpensive, more and more criminals leave digital trails. However, those trails commonly

---

\* J.D. Candidate, Northwestern University School of Law, 2011; B.S. University of Wisconsin-Madison. Special thanks to Professors Ronald J. Allen and Albert Alschuler for their help and feedback. Additional thanks to the past and present staff of the *Journal* for their ongoing fight against formatting errors, unsupported statements, and scrambled syntax.

lead through large databases, filled with data unrelated to any crime and bearing a high expectation of privacy. This poses a serious challenge to investigators attempting to retrieve the relevant data using a minimum amount of time and with the respect for the privacy of those searched that the Constitution requires. Because digital records are fungible and easily disguised or hidden, these searches sometimes require a file-by-file search of seized databases, forcing increased expenditures on conducting the search and increased privacy intrusions. This has challenged trial and appellate courts to develop a practical approach to preserving civil rights against unreasonable searches and unparticularized searches.

A recent en banc Ninth Circuit decision, *United States v. Comprehensive Drug Testing, Inc.*, attempted to do just that, adopting a series of procedural requirements for digital searches in criminal cases that appear to provide strong protections for digital privacy at the cost of placing a significant burden on the ability of law enforcement to pursue digital crimes.<sup>1</sup> This Comment will argue that, although digital searches raise valid Fourth Amendment concerns, the Ninth Circuit's approach is excessive and inefficient, and that a more flexible approach, based on the balancing of government interests, privacy interests, and the probability of a successful search, is preferable. Part II will review the facts and procedural history of *Comprehensive Drug Testing, Inc.* Part III will briefly revisit the history of the plain view doctrine and evaluate its applicability to digital searches. Part IV will discuss the variety of approaches proposed by other courts and scholars. Finally, Part V will argue that the most efficient approach to regulating digital searches is one where courts balance privacy interests with society's interests in detecting crime and encourage investigators to offer search methods that are respectful of privacy interests as well as reasonably efficient and effective. Ultimately, this Comment concludes that the *Comprehensive Drug Testing, Inc.* holding fails to strike a proper balance and is as a result impractical and inefficient.

## II. THE BALCO INVESTIGATION AND *COMPREHENSIVE DRUG TESTING, INC.*

In August 2002, the Internal Revenue Service's Criminal Investigations Unit began a grand jury investigation into the Bay Area Lab Cooperative (BALCO).<sup>2</sup> BALCO was a small lab which had several high-profile athletes as clients, including Barry Bonds, a Major League Baseball

---

<sup>1</sup> 579 F.3d 989 (9th Cir. 2009) (Kozinski, J.) (en banc), *rev'g* 473 F.3d 915 (9th Cir. 2006) (2-1).

<sup>2</sup> *United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915, 920 (9th Cir. 2006) [hereinafter *CDT I*]; MARK FAINARU-WADA & LANCE WILLIAMS, *GAME OF SHADOWS* 153 (2006).

player who hit a record seventy-three home runs during the 2001 season.<sup>3</sup> Federal investigators suspected that BALCO had provided Bonds and other athletes with performance-enhancing drugs.<sup>4</sup> They soon confronted the owner of BALCO, Victor Conte, who confessed to having developed and distributed two performance-enhancing drugs, known as “The Clear” and “The Cream.”<sup>5</sup> The investigation expanded its focus to the athletes who had been using those chemicals. A grand jury convened in September 2003 and began subpoenaing athletes with connections to BALCO.<sup>6</sup>

In November 2002, the Government served a grand jury subpoena on Major League Baseball (MLB), seeking drug testing information for ten players.<sup>7</sup> It also subpoenaed the records of the ten players from two drug testing companies retained by MLB to carry out its drug testing policies: Comprehensive Drug Testing, Inc. (CDT) and Quest Diagnostic Labs (Quest).<sup>8</sup> The Major League Baseball Players Association (Players Association) filed a motion to quash the subpoenas in the Northern District of California.<sup>9</sup>

While the Northern District considered that motion, the Government requested a search warrant from magistrate judges in the Central District of California and the District of Nevada.<sup>10</sup> The warrants authorized the seizure of drug test records and specimens for the ten BALCO-connected players, as well as materials explaining CDT’s procedure for administering the MLB drug-testing program, including correspondence and e-mails.<sup>11</sup> The Government executed the warrant at CDT, where it obtained records listing the players that CDT had tested along with the identifying numbers CDT used to label their documents and information.<sup>12</sup> A CDT director also provided the agents with a physical document that contained testing results

---

<sup>3</sup> FAINARU-WADA & WILLIAMS, *supra* note 2, at 153; *CDT I*, 473 F.3d at 920.

<sup>4</sup> FAINARU-WADA & WILLIAMS, *supra* note 2, at 153.

<sup>5</sup> *Id.* at 178. “The Clear” was a norbothenone, an obscure anabolic steroid not detected by most steroids tests at the time. *Id.* at 57. “The Cream” was a mix of testosterone and epitestosterone designed to conceal the use of norbothenone. *Id.* at 178.

<sup>6</sup> *Id.* at 190. The athletes came from a wide variety of sports including baseball, football, Olympic track and field, professional boxing, swimming, cycling, and bodybuilding. *Id.*

<sup>7</sup> *CDT I*, 473 F.3d at 920. The Government initially subpoenaed eleven players’ records, then notified CDT that they were no longer seeking records for one of those players. *Id.* at 920 n.7.

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

<sup>9</sup> *Id.* at 921. The decision also discussed the standing of the Players Association to sue on behalf of the players and MLB, but that subject is not otherwise discussed in this paper. *See id.* 925–26.

<sup>10</sup> *Id.* at 921.

<sup>11</sup> *Id.* at 924.

<sup>12</sup> *Id.* at 922.

for the ten BALCO players.<sup>13</sup> When another director informed the agents that the digital records of CDT's drug testing programs were maintained on a computer directory called the "Tracy" directory, an agent created a digital copy of the directory for analysis off-site.<sup>14</sup>

#### A. DISTRICT COURT

The Players Association filed a motion under Federal Rule of Criminal Procedure 41(g) in the Central District of California, asking for the return of the electronic records not related to the BALCO players.<sup>15</sup> The motion was granted by Judge Cooper, who rejected the Government's argument that the electronic documents seized were legally seized as plain view contraband and therefore not subject to a 41(g) motion.<sup>16</sup> The Players Association filed a similar order in the District of Nevada (where Quest is located), which was granted by Judge Mahan.<sup>17</sup> In granting the motion, Judge Mahan found that "[t]he government callously disregarded the affected players' constitutional rights" and had not followed the Ninth Circuit's procedural guidelines for searches of intermingled records laid out in *United States v. Tamura*.<sup>18</sup> He also found that the Government had misled the magistrate judge in obtaining the warrant by claiming that the records were in danger of being destroyed.<sup>19</sup>

#### B. COMPREHENSIVE DRUG TESTING INC. I

The Government appealed the orders of Judges Cooper and Mahon and the appeals were consolidated and heard by a Ninth Circuit panel.<sup>20</sup> The panel reversed the lower court orders.<sup>21</sup> The majority opinion held that the district court had improperly granted the 41(g) motions. It noted that

---

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

<sup>14</sup> *Id.* at 922–23.

<sup>15</sup> *Id.* at 923. FED. R. CRIM. P. 41(g) provides:

Motion To Return Property. A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

<sup>16</sup> *CDT I*, 473 F.3d at 924.

<sup>17</sup> *Id.*

<sup>18</sup> *Id.* The procedural requirements of *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), are discussed in more detail *infra* Part II.C.

<sup>19</sup> *CDT I*, 473 F.3d at 930.

<sup>20</sup> *Id.* at 915–16.

<sup>21</sup> *Id.* at 930.

the judges' orders, which required the return of *all* CDT and Quest records, were inconsistent with precedent.<sup>22</sup> It further noted that courts typically deny 41(g) motions in situations where "the government's need for the property as evidence continues" even though some unlawfully obtained evidence may be intermingled.<sup>23</sup> The panel also held that the *Tamura* procedures were "pragmatic" rather than constitutional in nature and thus not required.<sup>24</sup> The majority declined to decide whether or not the "plain view" exception to the warrant requirement was applicable, noting that the documents seized by the Government had been within the scope of their warrant.<sup>25</sup>

### C. COMPREHENSIVE DRUG TESTING, INC. II

The case was reheard en banc by the Ninth Circuit where, writing for the majority, Chief Judge Kozinski reversed the decision of the three-judge panel.<sup>26</sup> The opinion reviewed the Government's actions in the context of its previous decision, *United States v. Tamura*.<sup>27</sup> That case stemmed from a government kickback investigation into a manager (Tamura) at an American company.<sup>28</sup> The Government obtained a search warrant to seize particular records at the company.<sup>29</sup> The necessary records were intermingled with non-pertinent records and required a multi-step process to identify and segregate.<sup>30</sup> In order to avoid several days of searching for documents on-site, the Government decided to seize all of the corporation's records for the relevant time periods.<sup>31</sup> The search ultimately supplied evidence relevant to the investigation.<sup>32</sup> Tamura sought to suppress the evidence after the Government failed to return segregated non-pertinent files to the corporation.<sup>33</sup> The court held that the Government's "wholesale seizure" of documents not specified in the warrant constituted an

---

<sup>22</sup> *Id.* at 937.

<sup>23</sup> *Id.* (quoting *United States v. Fitzen*, 80 F.3d 387, 388 (9th Cir. 1996)).

<sup>24</sup> *Id.* at 938.

<sup>25</sup> *Id.* at 935 n.39.

<sup>26</sup> *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006–07 (9th Cir. 2009) (en banc) [hereinafter *CDT II*].

<sup>27</sup> *Id.* at 998 (citing *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982)).

<sup>28</sup> *Tamura*, 694 F.2d at 594.

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

<sup>30</sup> *Id.* at 594–95.

<sup>31</sup> *Id.* at 595. The court ultimately concluded that the Government's actions did not constitute a reversible error. *Id.* at 597.

<sup>32</sup> *Id.*

<sup>33</sup> *Id.* at 594–95.

“investigatory dragnet” prohibited by the Fourth Amendment.<sup>34</sup> The decision endorsed an approach described by the American Law Institute’s Model Code for Pre-Arrest Procedure, which states that once police seize intermingled documents, they are to be held under seal and cannot be searched until a neutral magistrate conducts a hearing on the least intrusive method for searching the files.<sup>35</sup>

The *Comprehensive Drug Testing, Inc.* en banc panel noted that the point of the *Tamura* procedures was to “maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search.”<sup>36</sup> It found that the Government’s decision to conduct a search of the entire hard drive with the discretion to exercise plain view was incompatible with this purpose.<sup>37</sup> Based on this observation and other issues related to the Government’s failure to appeal in a timely manner, the Ninth Circuit affirmed the district court orders.<sup>38</sup> In addition, in a section titled “Concluding Thoughts,” it laid out several holdings describing a set of procedures that magistrate judges and government investigators must “be vigilant in observing” when searching intermingled electronic data.

1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
2. Segregation and redaction must either be done by specialized personnel or an independent third party . . . . If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
4. The government’s search protocol must be designed to uncover only the information for which it has probable cause and only that information may be examined by the case agents.

---

<sup>34</sup> *Id.* at 595.

<sup>35</sup> *Id.* at 595–96 (citing Section SS 220.5 of the 1975 ALI MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE).

<sup>36</sup> *CDT II*, 579 F.3d 989, 998 (9th Cir. 2009).

<sup>37</sup> *Id.*

<sup>38</sup> *Id.* at 1007.

5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed when they have done so and what was kept.<sup>39</sup>

The *Comprehensive Drug Testing, Inc.* decision is a radical approach to maintaining the protections of the Fourth Amendment in a digital age and has attracted a significant amount of attention from legal commentators.<sup>40</sup>

---

<sup>39</sup> *Id.* at 1006 (internal citations omitted). Shortly prior to the publication of this Comment, the Ninth Circuit revisited its decision. *United States v. Comprehensive Drug Testing, Inc.*, Nos. 05-10067, 05-15006, 05-55354, 2010 WL 3529247 (9th Cir. Sept. 13, 2010), *revising and superceding* 579 F.3d at 989 [hereinafter *CDT III*]. The revised opinion, now per curiam, still reversed the *CDT I* opinion, however, much of Judge Kozinski's mandatory language was moved to a concurrence section, joined by Judges Kleinfeld, W. Fletcher, Paez, and M. Smith, indicating that Judges Graber, Wardlaw, and Berzon, had withdrawn their support for that section. *Id.* at \*1, \*14; *see also* Orin Kerr, *Ninth Circuit Balks in BALCO Case, Denying Super En Banc in United States v. Comprehensive Drug Testing but Amending Opinion to Remove Challenged Section*, THE VOLOKH CONSPIRACY (Sept. 13, 2010, 2:04 PM), <http://volokh.com/2010/09/13/ninth-circuit-balks-in-balco-case-denying-super-en-banc-in-united-states-v-comprehensive-drug-testing-but-amending-opinion-to-remove-challenged-section/>. In the new opinion, Judge Kozinski recharacterized the guidance procedures as a “safe harbor” for government searches. *CDT III*, 2010 WL 3529247 at \*14. Nonetheless, the concurrence implies that a failure to follow the guidance would result in a “significant” decrease in the odds of a district or magistrate judge’s warrant being deemed reasonable. *See id.* (“[H]eeding this guidance will significantly increase the likelihood that the searches and seizures of electronic storage that they authorize will be deemed reasonable and lawful.”). The holding, as revised, is now somewhat ambiguous. Read narrowly, the *Comprehensive Drug Testing, Inc.* decision now stands primarily on the failure of the Government to comply with the *Tamura* procedures, which themselves preclude “plain view” as a justification for seizure. *Id.* at \*6. What remains unclear is what specific set of circumstances trigger *Tamura* procedures. Clearly, seizure of intermingled documents in the possession of a third party will be certain to trigger *Tamura*, since those were the circumstances of both *Tamura* and *Comprehensive Drug Testing, Inc.* But the court implies that it might also be triggered in first-party instances, since it cites to *United States v. Hill*, 322 F. Supp. 2d 1081 (C.D. Cal. 2004), which was such a case. *Id.* at \*6. Alternatively, *Tamura* may be triggered by the removal of intermingled documents to a government facility. *See CDT III*, 2010 WL 3529247 at \*5 (“No doubt in response to [the *Tamura* precedent], the government here did seek advance authorization for sorting and segregating the seized materials off-site.”). However, whether or not this disincentivization of removal will solve the Fourth Amendment challenge posed by digital evidence seems unclear, and the decision may simply encourage the government to engage in on-site digital forensic investigations whenever possible in order to avoid triggering *Tamura* procedures.

<sup>40</sup> *See, e.g.*, Recent Case, *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (*en banc*), 123 HARV. L. REV. 1003 (2010); John R. Emshwiller, *Currents—Law Journal: Courts Wrestle with Searches When the Evidence Is Digital*, WALL ST. J., Sept. 24, 2009, at A17 (“A recent ruling by the federal Ninth Circuit Court of Appeals addressed this question, and the decision could reshape what government investigators can—and can’t—do when searching digital devices for evidence of crime.”); *Welcome to the Digital Fourth*, SIMPLE JUSTICE, (Aug. 28, 2009), <http://blog.simplejustice.us/2009/08/28/welcome-the-digital-fourth.aspx>; Ashby Jones, *Beyond A-Rod and ManRam: Plain Talk on*



Its holdings attempt to create a firewall between investigators and digital information not specified in the warrant. By forcing investigators to waive plain view claims, it seeks to further ensure that evidence of crimes discovered during a digital search will only be admitted if the evidence was described with particularity in the warrant. Further still, by requiring the search to be conducted by a technician sworn to secrecy, it creates an additional barrier to the use of plain view to justify seizures since information not particularized in the warrant never reaches investigators. Instead, the non-pertinent information (no matter how incriminating) is limited to the specialists, who must disregard it. It also demands that magistrate judges be presented with search protocols designed to uncover “only” the information sought, although it is unclear how literally this holding is to be interpreted.<sup>41</sup>

Judge Kozinski’s decision reflects a sharp skepticism towards the use of digital plain view, which may reflect a general concern that “plain view is killing the Fourth Amendment” in general.<sup>42</sup> The *Comprehensive Drug Testing, Inc.* holding represents a much more aggressive response to the Fourth Amendment implications of computer searches than the decisions from any other federal court and carries serious implications.<sup>43</sup> Forcing government agents to waive plain view arguments may lead to serious crimes going unprosecuted. The other procedures dictated by the holding

---

the ‘Plain View Doctrine,’ WALL ST. J. L. BLOG (Aug. 28, 2009, 12:40 AM), <http://blogs.wsj.com/law/2009/08/28/beyond-a-rod-and-manram-plain-talk-on-the-plain-view-doctrine/> (reprinting comments of Professor Peter Henning) (“While I suspect prosecutors can live with the other requirements the Ninth Circuit imposed, giving up the plain view doctrine is going to be a non-starter. That requirement may well cause the government to take the case to the Supreme Court.”); Orin Kerr, *Ninth Circuit Enacts Miranda-Like Code for Computer Search and Seizure*, THE VOLOKH CONSPIRACY, (Aug. 26, 2009, 1:38pm), <http://volokh.com/posts/1251308337.shtml>.

<sup>41</sup> The *Comprehensive Drug Testing, Inc.* decision represents a fairly clear break with prior Ninth Circuit precedents. Judge Callahan, writing in dissent, catalogued several. *CDT II*, 579 F.3d 989, 1010 (9th Cir. 2009) (Callahan, J., dissenting) (citing *United States v. Giberson*, 527 F.3d 882, 887–88 (9th Cir. 2008) (declining to impose heightened Fourth Amendment protections in computer search cases as a result of a computer’s ability to store large amounts of potentially intermingled information, and stating that such heightened protections must be “based on a principle that is not technology-specific”); *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006) (upholding digital plain view when seizure of hardware was supported by a reasonable explanation); *United States v. Wong*, 334 F.3d 831, 837 (9th Cir. 2003)).

<sup>42</sup> See *United States v. Lemus*, 569 F.3d 512, 516 (9th Cir. 2010) (denying en banc appeal) (Kozinski, J., dissenting) (“Plain view is killing the Fourth Amendment. Because our plain-view case law is so favorable to the police, they have a strong incentive to maneuver into a position where they can find things in plain view, or close enough to lie about it.”).

<sup>43</sup> See *infra* Part IV.A.

have invited comparisons to the complex procedural requirements of *United States v. Miranda*,<sup>44</sup> and have been enacted with little mention of practicality.<sup>45</sup> To help place this decision in context, a brief summary of plain view doctrine and the approaches to digital searches adopted by other courts follows.

### III. PLAIN VIEW DOCTRINE AND SEARCHES

Plain view doctrine is a longstanding concept within search and seizure law.<sup>46</sup> It is one of several exceptions to the Fourth Amendment, which requires warrants in most searches and seizures.<sup>47</sup> The exception permits warrantless seizure of evidence that is: (1) found during a prior justified intrusion; (2) in plain view; and (3) incriminating in a manner that is “immediately apparent.”<sup>48</sup> It is “grounded on the proposition that once police are lawfully in a position to observe an item first-hand, its owner’s privacy interest in that item is lost; the owner may retain the incidents of title and possession but not privacy.”<sup>49</sup> Since plain view is at the core of the Ninth Circuit’s concerns regarding digital searches, a brief review follows.

#### A. COOLIDGE V. NEW HAMPSHIRE

One of the earliest cases clearly defining and justifying the plain view doctrine is *Coolidge v. New Hampshire*.<sup>50</sup> The case dealt with the seizure

---

<sup>44</sup> Kerr, *supra* note 40.

<sup>45</sup> See Brief of Plaintiff-Appellant at 15–18, *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (Nos. 05-10061, 05-15006, 05-55354) (providing a discussion of the difficulties of applying the case officer technician firewall).

<sup>46</sup> See, e.g., *Entick v. Carrington*, 19 How. St. Tr. 1026, 1066 (1765) (Lord Camden) (“[T]he eye cannot by the laws of England be guilty of a trespass.”).

<sup>47</sup> U.S. CONST. amend. IV. See generally *United States v. Leon*, 468 U.S. 897 (1984) (good faith error); *Florida v. Bostick*, 501 U.S. 429 (1991) (consent); *Hester v. United States* 265 U.S. 57 (1987) (open fields doctrine); *United States v. Santana*, 427 U.S. 38 (1976) (exigent circumstances); *Terry v. Ohio* 392 U.S. 1 (1968) (stop and frisk exception); *Warden v. Hayden*, 387 U.S. 294, 298–300 (1967) (“hot pursuit” of fleeing suspect); *Schmerber v. California*, 384 U.S. 757 (1966) (imminent destruction of evidence); *Carroll v. United States*, 267 U.S. 132, 153 (1925) (automobile exception); see also THOMAS N. MCINNIS, *THE EVOLUTION OF THE FOURTH AMENDMENT* 8–9, 75–114 (2009) (listing the recognized exceptions to the warrant requirement and attributing their development as a response to the creation of the exclusionary rule in *Mapp v. Ohio*, 367 U.S. 643 (1961)).

<sup>48</sup> See Howard E. Wallin, *Plain View Revisited*, 22 PACE L. REV. 307, 307 (2002) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 446 (1971)).

<sup>49</sup> *Illinois v. Andreas*, 463 U.S. 765, 771 (1983).

<sup>50</sup> 403 U.S. at 443. The Court had previously decided several cases permitting police to lawfully seize articles of an “incriminating character” not specified in the warrant being executed. *Id.* at 465 (citing *Stanley v. Georgia*, 394 U.S. 557, 571 (1969) (Stewart, J.,

of a car on the property of a murder suspect.<sup>51</sup> The Court held that the “plain view” doctrine permits unwarranted seizures of clearly incriminating evidence under certain circumstances.<sup>52</sup> The Court justified this principle by first noting that the warrant requirement serves two specific purposes: eliminating searches not based on probable cause and limiting searches such that the warrants do not resemble the colonial practice of issuing “general warrants.”<sup>53</sup> It reasoned that permitting the seizure of objects in plain view does not violate the first objective, since the view is predicated on the exercise of a lawfully obtained search warrant based on probable cause.<sup>54</sup> It then reasoned that the second objective was also satisfied because the initial intrusion was justified by a particularized warrant and plain view does not otherwise convert the search into a general warrant.<sup>55</sup> However, plain view searches could not be used “to extend a general exploratory search from one object to another until something incriminating at last emerges.”<sup>56</sup>

In *Coolidge*, the Court also adopted an “inadvertence” requirement, requiring that evidence seized under plain view be discovered accidentally rather than intentionally.<sup>57</sup> Justice Black criticized the inadvertence rule in his concurrence,<sup>58</sup> arguing that the “reasonableness” of a search should be evaluated “under all the circumstances” rather than by affixing per se rules.<sup>59</sup> Justice Black’s position on the inadvertence requirement would ultimately be adopted by the Court in *California v. Horton*.<sup>60</sup> Noting that the discussion of “inadvertence” was limited to the plurality opinion, the Court declined to apply it to the present case.<sup>61</sup> Its two primary criticisms

---

concurring in result)); *United States v. Lefkowitz*, 285 U.S. 452, 465 (1932); *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 358 (1931); *Steele v. United States*, 267 U.S. 498 (1925). *Coolidge* is noteworthy for first establishing “plain view” as a distinct legal doctrine. 403 U.S. at 443.

<sup>51</sup> *Id.* at 445.

<sup>52</sup> *Id.* at 465.

<sup>53</sup> *Id.* at 467; see also WILLIAM CUDDIHY, *FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING* 602–1791, at 569–74 (2009).

<sup>54</sup> *Coolidge*, 403 U.S. at 467.

<sup>55</sup> *Id.* at 467.

<sup>56</sup> *Id.* at 466.

<sup>57</sup> *Id.* at 469.

<sup>58</sup> *Id.* at 506–07 (Black, J., concurring and dissenting).

<sup>59</sup> *Id.* at 509–10.

<sup>60</sup> 496 U.S. 128 (1990). The case stemmed from the execution of a search warrant based on probable cause of robbery and only authorizing a search of the defendant’s house for the proceeds of that robbery. Instead the searching officer discovered weapons in plain view, which were seized as evidence. *Id.* at 131.

<sup>61</sup> *Id.* at 136–37.

were: (1) that objective standards were preferable to standards that “depend on the subjective state of mind of the officer” and, (2) because the particularity requirement of the Fourth Amendment was sufficient to protect against the danger of general warrants, the additional protection of an inadvertence requirement was unnecessary.<sup>62</sup>

#### B. ARIZONA V. HICKS

In *Arizona v. Hicks* the Supreme Court clarified plain view doctrine by requiring probable cause for plain view evidence to be seized.<sup>63</sup> In that case, officers entered an apartment without a warrant in response to a shot fired from that apartment into the one below.<sup>64</sup> Upon entering the apartment, they discovered an expensive stereo component that, given the seemingly “squalid” condition of the apartment as a whole, fell under immediate suspicion of being stolen.<sup>65</sup> An officer moved the stereo component in order to view the serial number, which was used to confirm that it was, in fact, stolen.<sup>66</sup>

The Court held that the moving of the stereo component constituted an unreasonable search.<sup>67</sup> Even though the invasion of privacy was simply moving a stereo component “a few inches,” the Court drew a bright line.<sup>68</sup> Since the gun that the officers were authorized to search for could not have been located in the area underneath the stereo component, the warrantless search of the stereo was unreasonable.<sup>69</sup> Even though the officer had a reasonable suspicion to believe that the stereo was stolen, he lacked probable cause and so was prohibited from “seizing” the turntable in order

---

<sup>62</sup> *Id.* at 138–40.

<sup>63</sup> 480 U.S. 321 (1987). The requirement of probable cause has been explicitly left unresolved in cases such as *Texas v. Brown*, 460 U.S. 730, 742 n.7 (1983) (plurality). See also Wallin, *supra* note 48, at 311–15 (discussing how the ambiguity of pre-*Hicks* caselaw led to some lower courts adopting standards lower than probable cause).

<sup>64</sup> *Hicks*, 480 U.S. at 323.

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

<sup>66</sup> *Id.* at 323–34.

<sup>67</sup> *Id.* at 328.

<sup>68</sup> *Id.* at 325.

<sup>69</sup> *Id.* at 325–26. The ruling also corrected an interpretation of *Coolidge* put forward by the Arizona Court of Appeals. *State v. Hicks*, 707 P.2d 331 (Ariz. Ct. App. 1985). The Arizona court had held in *Hicks* that the search was unreasonable because the turntable was unrelated to the shooting that justified the warrantless entry into the apartment. This implied that even if the serial number had been on the top of the turntable and plainly visible, the search would have been unreasonable. The Supreme Court directly rejected this interpretation. *Hicks*, 480 U.S. at 325.

to view its serial number.<sup>70</sup> Since the officer only had a “reasonable suspicion” that the stereo component was stolen, the Court held that probable cause was lacking and an additional warrant would have been required.<sup>71</sup>

### C. DIGITAL PLAIN VIEW<sup>72</sup>

The Supreme Court’s treatment of plain view and plain view analogues seems to be driven by a desire to prevent “fishing expeditions” and dragnets, but to also create objective working rules for defining what a “fishing expedition” is, rather than the simpler—but rightfully abandoned—approach of asking whether or not the officer subjectively believed that he was engaged in a fishing expedition. In physical cases, these fishing expeditions can be detected by a sort of common sense reasoning. An officer who detects contraband through “plain feel” while conducting a legitimate *Terry* search is thus judged to be conducting a legitimate search,<sup>73</sup> while an officer who boards a bus and squeezes soft-shell luggage until contraband is discovered is not.<sup>74</sup> The judge is supposed to look at the surrounding context of the officer’s actions and judge its reasonableness.

One of the central problems raised by digital plain view is that this common sense reasoning becomes more difficult to apply in a digital context. Digital searches take place in an abstract space and the intentions of officers conducting such a search can be difficult to objectively determine, except in the most blatant cases. In *Hicks*, the shifting of the stereo equipment, even though it was a minor act by the officer, clearly raised a flag for the Court, since it was clear that the act was unrelated to searching for a gun. By contrast, the actions of officers searching a computer might not always be as easily reviewed by the courts for blatant Fourth Amendment violations. This dynamic is concerning, since it makes policing the execution of digital search warrants more difficult at the same time as those warrants offer improved opportunities for fishing expeditions.

---

<sup>70</sup> *Hicks*, 480 U.S. at 322, 326–27 (noting that the exceptions are for circumstances where the seizure is “minimally intrusive and operational necessities render it the only practicable means of detecting certain types of crime”).

<sup>71</sup> *Id.* at 322, 326.

<sup>72</sup> This Comment will use the term “digital plain view” to refer to any evidence encountered while searching digital media that, while not responsive to the warrant permitting the search, is nonetheless seizable in a manner similar to evidence encountered in traditional plain view situations such as *Coolidge v. New Hampshire*, 403 U.S. 443 (1971).

<sup>73</sup> *Minnesota v. Dickerson*, 508 U.S. 366, 370–71 (1993).

<sup>74</sup> *Bond v. United States*, 529 U.S. 334, 336 (2000).

But, in holding that the use of plain view in digital searches is *per se* unconstitutional, the *Comprehensive Drug Testing, Inc.* decision is inconsistent with existing Supreme Court precedent. Allowing the use of digital evidence discovered in plain view satisfies the first two purposes of the warrant requirement, as defined in *Coolidge*. First, a digital plain view claim does not waive the probable cause requirement any more than a conventional plain view claim does.<sup>75</sup> Indeed, maintaining the probable cause requirement is essential to the approach advocated in this Comment, since it provides a critical point of reference for judges seeking to objectively assess the reasonableness of search warrants.<sup>76</sup> Second, a properly particularized search warrant does not constitute a “general warrant.” Typically, courts have not found that searches limited to a particular place, in pursuit of a particular crime, and seeking sufficiently particularized items constitute general warrants.<sup>77</sup> Digital plain view, despite the dangers, can be made to work if the courts are provided a new way of objectively assessing whether the search being conducted is reasonable, or simply an opportunistic fishing expedition.

#### IV. SEARCHES OF DIGITAL DATABASES

No court has attempted as detailed an approach to regulating digital searches as the Ninth Circuit. The district courts have generally been free to develop their own approaches, although they have generally been fairly permissive of digital searches. Digital search problems have also attracted the attention of many legal scholars whose proposals and solutions have found their way into the reasoning of some courts. This section surveys these approaches.

---

<sup>75</sup> *Cf. Hicks*, 480 U.S. at 326 (1987).

<sup>76</sup> *See infra* Part V.

<sup>77</sup> *See Coolidge*, 403 U.S. at 467 (“[T]he problem [posed by the general warrant] is not that of intrusion *per se*, but of a general, exploratory rummaging in a person’s belongings . . . . [The Fourth Amendment addresses the problem] by requiring a particular description of the things to be seized.”); *United States v. Cioffi*, 668 F. Supp. 2d 385, 392 (E.D.N.Y. 2009) (“[A]uthorization to search for ‘evidence of a crime,’ that is to say, any crime, is so broad as to constitute a general warrant.”) (quoting *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992)); *see also* *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 301 (1967) (noting that the general warrants permitted searches under “indiscriminate, general authority” and that the Fourth Amendment ended general searches by requiring that the warrant “particularly describe the place to be searched, and the persons or things to be seized”) (internal quotations omitted); *United States v. Mankani*, 738 F.2d 538, 546 (2d Cir. 1984) (holding that a warrant whose terms authorized seizure of documents “pertaining to a specific fraudulent transaction and a specific piece of real estate” did not constitute a general warrant).

## A. CIRCUIT COURT DECISIONS

Both circuit and district courts have addressed the question of the application of plain view to digital database searches. While there has been some variation, most have permitted digital searches using plain view when the data was incriminating and discovered while executing a particularized warrant based on probable cause.

*I. United States v. Carey: The File-Based Approach*

In *United States v. Carey*, the Tenth Circuit reviewed a case in which the police executed a search warrant for evidence of the sale and possession of cocaine by the defendant.<sup>78</sup> Upon discovering computers on the premises, the officers seized them and obtained an additional search warrant to search the hard drives for “names, telephones, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.”<sup>79</sup> The police technician first attempted to search for key words related to drug sales in “text-based” files.<sup>80</sup> When that failed, he “explore[d]” the computer until he discovered a particular image file, which he proceeded to open.<sup>81</sup> It contained child pornography. Rather than obtaining a warrant expanding the scope of the search, the officer continued opening files in that directory.<sup>82</sup> Many of those files contained additional images of child pornography and were labeled with sexually suggestive titles.<sup>83</sup>

The court held that the search of image files beyond the first file was unreasonable.<sup>84</sup> It noted that after opening the first file, the officer, by his own admission, had probable cause to believe that the remaining files in the directory also contained child pornography rather than evidence of drug distribution.<sup>85</sup> Citing *Tamura*, it held that in computer searches, officers must conduct an “intermediate step” and attempt to sort the digital files such that intermingled non-pertinent files are removed prior to the search beginning in earnest.<sup>86</sup> It also directed that magistrates “should” require the officers to specify which types of files are sought.<sup>87</sup>

---

<sup>78</sup> 172 F.3d 1268, 1270 (10th Cir. 1999).

<sup>79</sup> *Id.*

<sup>80</sup> *Id.* at 1271.

<sup>81</sup> *Id.*

<sup>82</sup> *Id.*

<sup>83</sup> *Id.* at 1271 & n.3.

<sup>84</sup> *Id.* at 1276–77.

<sup>85</sup> *Id.* at 1274.

<sup>86</sup> *Id.* at 1275 (citing *United States v. Tamura*, 694 F.2d 591, 595–96 (9th Cir. 1982)).

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

This file-based approach to regulating digital searches has not found much success as courts have become more aware of the ease with which it can be circumvented.<sup>88</sup> The Tenth Circuit has already begun to walk away from the *Carey* holding, noting in subsequent cases that it was a “limited” and “fact-intense” holding<sup>89</sup> that “simply stands for the proposition that law enforcement may not expand the scope of a search beyond its original jurisdiction.”<sup>90</sup> Although the Tenth Circuit seems to be in the process of marginalizing *Carey*, it remains influential in some circuit court decisions.<sup>91</sup> However, the acceptance is far from universal.

## 2. United States v. Mann: *The Ambiguous Scrutiny Approach*

Subsequent to the *Comprehensive Drug Testing, Inc.* decision, the Seventh Circuit has approved the use of digital plain view.<sup>92</sup> That case, *United States v. Mann*, concerned the warranted seizure and search of a hard drive that the police believed contained evidence related to the defendant’s covert videotaping of a high school locker room.<sup>93</sup> Upon searching the hard drive using specialized software, the police discovered “many, many images of child pornography” as well as videos of the locker room.<sup>94</sup> The defendant moved to suppress the evidence, arguing that the

---

<sup>88</sup> See, e.g., *United States v. Williams*, 592 F.3d 511, 522–23 (4th Cir. 2010) (noting that *Carey* seems to establish an inadvertence requirement which is difficult to reconcile with the holding of *Horton v. California*, 496 U.S. 128, 136–37 (1990)).

<sup>89</sup> *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir. 2009).

<sup>90</sup> *United States v. Grimm*, 439 F.3d 1263, 1268 (10th Cir. 2006).

<sup>91</sup> See *infra* note 111.

<sup>92</sup> *United States v. Mann*, 592 F.3d 779, 785 (7th Cir. 2010) (citing *CDT II*, 579 F.3d 989 (9th Cir. 2009)). Although the *Mann* decision was released after *Comprehensive Drug Testing, Inc.*, it only contains one passing reference to *CDT II*. *Id.* The Seventh Circuit had previously addressed the question of plain view in dicta. *United States v. Raney*, 342 F.3d 551, 558–59 (7th Cir. 2003) (upholding search on grounds that the data seized was particularized in the warrant, but alternatively permitted under plain view).

<sup>93</sup> *Mann*, 592 F.3d at 780.

<sup>94</sup> *Id.* at 781. Some of the child pornography had been discovered using a “hashing” program, an automated program that can detect the presence of a particular file on a computer hard drive if the exact digital contents of that file are already known to the investigators. See Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL’Y 2 (2007); see also *United States v. Gabel*, No. 10-60168, 2010 U.S. Dist. LEXIS 107131, at \*8–9 (S.D. Fla. Sept. 16, 2010) (describing the national database of “child notable” image files, which investigators use to program the automated hashing programs). The court ultimately suppressed the files discovered by the hashing program, because it targeted known child pornography files, even though the search was for files with unknown digital contents. *Mann*, 592 F.3d, at 784–85. The *Comprehensive Drug Testing, Inc.* en banc decision also expressed concern, in dicta, about the use of hashing programs. *CDT II*, 579 F.3d at 999. However, hashing programs



police had exceeded the scope of their warrant and had effectively conducted a prohibited general search.<sup>95</sup>

The court upheld the search, noting that the software used by the officer served primarily to collect image files, including disguised files, and display them.<sup>96</sup> The court noted that the warrant directed the police to search “places likely to contain ‘images of women in locker rooms and other private places,’” and that such an image file could be hidden virtually anywhere within the computer.<sup>97</sup> Since the program was used in a “systematic” way to search the computer, the discovery and seizure of child pornography was reasonable.<sup>98</sup> The court specifically declined to adopt the holding of *Comprehensive Drug Testing, Inc.*, instead adopting Judge Callahan’s criticism that the abolition of digital plain view was an “efficient but overbroad approach.”<sup>99</sup> The court counseled that magistrates “exercise caution to ensure” that digital search warrants meet the particularity requirement and are narrowly tailored.<sup>100</sup> It is difficult to know what this “narrowly tailored” requirement consists of, since the court approvingly cited *United States v. Gray*.<sup>101</sup> In that case, digital plain view was held to justify the discovery of child pornography during a file-by-file search of a computer due to the fact that the search was done systematically and

---

raise interesting questions in light of Supreme Court precedents, such as *United States v. Jacobsen*, in which the Court upheld a government chemical test for the presence of cocaine in a pile of white powder that fell out of an in-transit delivery package. 466 U.S. 109 (1984). The warrantless search was upheld because it could disclose no “private facts,” only the presence of cocaine. *Id.* at 123 (“A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy.”). What limits therefore should be placed on hashing programs, even if they are undeniably used to conduct warrantless fishing expeditions? See *United States v. Borowy*, 595 F.3d 1045, 1048 n.2 (9th Cir. 2010) (suggesting that using hashing software to “vacuum[] vast quantities of [internet] data indiscriminately” may result in a Fourth Amendment violation, but upholding its use to detect child pornography shared using peer-to-peer software); *United States v. Richardson*, 583 F. Supp. 2d 694 (W.D. Pa. 2008) (invalidating hash program search on grounds that the search was directed towards child pornography, but the officers lacked a warrant and had only been given consent by owner to search for evidence of “illegal credit card use”). For a broader discussion of the “private facts” model discussed in *Jacobsen*, see Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 512 (2007); see also James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 387–90 (2002) (criticizing the *Jacobsen* decision’s rationale).

<sup>95</sup> *Mann*, 592 F.3d at 782.

<sup>96</sup> *Id.* at 785–86.

<sup>97</sup> *Id.* at 782.

<sup>98</sup> *Id.* at 786.

<sup>99</sup> *Id.* at 785.

<sup>100</sup> *Id.* at 786.

<sup>101</sup> *Id.* at 784.

regardless of file name.<sup>102</sup> Thus, the court's directive to narrowly tailor searches clearly still allows law enforcement to conduct searches of entire hard drives, while adopting *Carey*-like requirement of a systematic search.

### 3. United States v. Williams: *The Status Quo Approach*

The facts of *United States v. Williams* resembled those of *Mann*, although *Williams* stemmed from an investigation into threatening e-mails sent to a church rather than voyeurism.<sup>103</sup> The police obtained a broad warrant, authorizing the seizure of “[a]ny and all computer systems and digital storage media, videotapes, videotape recorders, documents, photographs, and Instrumentalities indicat[ive] of [criminal e-mail harassment].”<sup>104</sup> Searches of these media uncovered child pornography, some of it placed in files mislabeled “Virus Shield Quaranteed [sic] Files, Destroy.”<sup>105</sup>

The Fourth Circuit upheld the application of plain view, applying a more permissive approach to digital searches than the Seventh Circuit. In a sort of preamble, the court announced its expectation that digital searches and seizures would soon develop a “set of rules . . . that attempts to achieve the same purpose [as the rules for physical searches] in a very different factual context.”<sup>106</sup> However, the court rejected the specific argument presented, which was that the immense amount of data stored on computers created a heightened expectation of privacy, requiring specialized requirements for searches under the Fourth Amendment.<sup>107</sup> The court refused to treat digital databases in a manner different than a file cabinet containing a large number of documents.<sup>108</sup>

Although the court recognized the “grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers,”<sup>109</sup> it noted that these concerns simply “counsel[] care and respect for privacy when executing a warrant” and do not prevent lawful searches

---

<sup>102</sup> *Id.* (citing *United States v. Gray*, 78 F. Supp. 2d 524, 527 (E.D. Va. 1999) (upholding the opening of a file labeled “tiny teen” by an officer searching for evidence of computer hacking because officer opened the file only after opening every file listed previous to it in the file directory)).

<sup>103</sup> 592 F.3d 511, 514–15 (4th Cir. 2010). The threats to the church made mention of a desire to molest young boys who attended the church. *Id.*

<sup>104</sup> *Id.* at 515.

<sup>105</sup> *Id.* at 516.

<sup>106</sup> *Id.* at 515.

<sup>107</sup> *Id.* at 518.

<sup>108</sup> *Id.* at 523.

<sup>109</sup> *Id.* (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)).

of computer files.<sup>110</sup> Because the court accepted the logic that files may be mislabeled, as the files were in this case, the file-by-file search conducted met the requirements of plain view once the “immediately apparent” child pornography came into view.<sup>111</sup> Since the search complied with the basic requirements for searches of physical documents, the court ultimately upheld the search.<sup>112</sup> Despite being decided several months after *Comprehensive Drug Testing, Inc.*, the decision did not mention the case, although it did cite to a prior Ninth Circuit decision, *United States v. Giberson*, which similarly held that for the purposes of the Fourth Amendment, digital storage media are not significantly different than other closed containers.<sup>113</sup>

#### B. DISTRICT COURT DECISIONS

The district courts have been addressing issues raised by plain view digital searches for over a decade.<sup>114</sup> As one might expect, they have adopted a range of approaches. For example, in *United States v. Fumo*, a case in the Eastern District of Pennsylvania, the court adopted a pro-search approach to digital records, noting that “because of the nature of computer files, the government may legally open and briefly examine the nature of each file when searching a computer pursuant to a valid warrant.”<sup>115</sup>

Like the Fourth Circuit, the district courts have generally rejected the position that, by their nature, digital records must be protected in a different

---

<sup>110</sup> *Id.* at 523–24.

<sup>111</sup> *Id.* at 522–23.

<sup>112</sup> *Id.* at 524.

<sup>113</sup> *Id.* (citing *United States v. Giberson*, 527 F.3d 882 (9th Cir. 2008)). The court cited *Giberson* in support of its treatment of computers as a container. *Id.*

<sup>114</sup> See generally *United States v. Kim*, 677 F. Supp. 2d 930 (S.D. Tex. 2009); *United States v. Farlow*, No. CR-09-38-B-W, 2009 WL 4728690 (D. Me. Sep. 29, 2009); *United States v. Cioffi*, 668 F. Supp. 2d 385 (E.D.N.Y. 2009); *United States v. Crespo-Rios*, 623 F. Supp. 2d 198 (D.P.R. 2009); *United States v. Mann*, No. 2:07-CR-197, 2008 WL 1701743, (N.D. Ind. April 8, 2008); *United States v. Richardson*, 583 F. Supp. 2d 694 (W.D. Pa. 2008); *United States v. Fumo*, 565 F. Supp. 2d 638 (E.D. Pa. 2008); *United States v. Sage*, Crim. Act. No. 07-00006-01-CR-W-SOW, 2007 LEXIS 99110 (W.D. Mo. Dec. 3, 2007); *United States v. Kearns*, No. 1:05-CR-146-WSD-JMF, 2006 WL 2668544 (N.D. Ga. Feb. 21, 2006); *United States v. Kaechele*, 466 F. Supp. 2d 868 (E.D. Mich. 2006); *United States v. Welch*, 401 F. Supp. 2d 1172 (D. Kan. 2005); *United States v. Hill*, 322 F. Supp. 2d 1081 (C.D. Cal. 2004); *United States v. Maali*, 346 F. Supp. 2d 1226 (M.D. Fla. 2004); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 961–62 (N.D. Ill. 2004); *United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31 (D. Conn. 2002); *United States v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999); *United States v. Hunter*, 13 F. Supp. 2d 574 (D. Vt. 1998).

<sup>115</sup> *Fumo*, 565 F. Supp. 2d at 649.

manner than physical records.<sup>116</sup> The decisions tend to reject arguments claiming overbroad searches<sup>117</sup> or unparticularized warrants.<sup>118</sup> While at least one court has experimented with requiring the government to provide search protocols,<sup>119</sup> only a few cases have analyzed the case using the *Carey* file-based framework<sup>120</sup> and many have distinguished or rejected it.<sup>121</sup>

One case addressing the issue of search methodology is *United States v. Hill*.<sup>122</sup> The case is of particular note as it was decided by Judge Kozinski, sitting by designation as a district court judge, five years prior to authoring the *Comprehensive Drug Testing, Inc.* decision. The case, like many digital search cases, involved a suppression motion filed by a defendant in a child pornography possession case. The suppression motion argued, in part, that the search warrant granted to the police for digital storage media was overbroad because it failed to define a search methodology based on file names or types. Judge Kozinski rejected this argument, noting that “images can be hidden in all manner of files, even

---

<sup>116</sup> See *United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, at \*36 (S.D.N.Y. Apr. 5, 2007) (“At bottom . . . there is neither a heightened nor a reduced level of protection for information stored on computers, as there is no justification for favoring those who are capable of storing their records on computer over those who keep hard copies of their records.”); *accord Hunter*, 13 F. Supp. 2d at 584; *Gray*, 78 F. Supp. 2d at 524.

<sup>117</sup> See *United States v. Jack*, No. CR.S-07-0266 FCD, 2009 WL 453051, at \*4 (E.D. Cal. Feb. 23, 2009) (providing a list of district and circuit court cases rejecting or discounting these overbreadth arguments). *But see Richardson*, 583 F. Supp. 2d at 964 (suppressing image files in “plain view” during a consented to search when the search would only require searching text or internet-based files).

<sup>118</sup> See *Sage*, 2007 LEXIS 99110 at \*18; *Farlow*, 2009 WL 4728690 at \*5. *But see Mink v. Knox*, 2010 U.S. App. LEXIS 14684 (10th Cir. July 19, 2010) (rejecting search warrant on particularity grounds, since the warrant failed to specify the crime that investigators were to search the computer for evidence of).

<sup>119</sup> See *In re Search of 3817 W. West End*, 321 F. Supp. 2d at 961 (requiring “as a practical matter” that the Government provide magistrates with search protocols when searching intermingled digital documents in order to satisfy the particularity requirement of the Fourth Amendment); *see also United States v. Barbuto*, No. 2:00CR197K, 2001 WL 670930, \*4 (D. Utah Apr. 13, 2001) (holding that methods or criteria by which a search of computer files would be conducted “should have been presented to [a] . . . magistrate before the issuance of the warrants or to support the issuance of a second, more specific warrant once intermingled documents were discovered”).

<sup>120</sup> See *Mann v. United States*, 592 F.3d 779, 783–84 (7th Cir. 2010); *Richardson*, 583 F. Supp. 2d at 716.

<sup>121</sup> *United States v. Kim*, 677 F. Supp. 2d 930, 948 (S.D. Tex. 2009); *Jack*, 2009 WL 453051, at \*4; *United States v. Kearns*, No. 1:05-CR-146-WSD-JMF, 2006 WL 2668544, at \*7 (N.D. Ga. Feb. 21, 2006); *United States v. Welch*, 401 F. Supp. 2d 1172, 1179 (D. Kan. 2005); *Gray*, 78 F. Supp. 2d at 530.

<sup>122</sup> 332 F. Supp. 2d 1081 (C.D. Cal. 2004).

word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.”<sup>123</sup> Ultimately, the search was upheld.<sup>124</sup>

The district courts have been weighing the reasonableness of digital plain view for some time, experimenting with different methods for evaluating the reasonableness of search warrant applications based on their knowledge of existing technology and circuit court methods. Although their results have produced variation, their collective experience indicates that they could cope with a more flexible approach to reviewing digital search applications than the one advocated in *Comprehensive Drug Testing, Inc.*

### C. SCHOLARLY WRITING

Digital searches have attracted the attention of legal scholars for well over a decade. Published articles have advocated a variety of positions, from abolition of plain view to unfettered continuation.<sup>125</sup> The articles have

---

<sup>123</sup> *Id.* at 1090.

<sup>124</sup> *Id.* Judge Kozinski’s decision in *United States v. Hill* is very difficult to reconcile with his stance in *Comprehensive Drug Testing, Inc.* One difference (among others) was that *Hill* concerned the privacy of a child pornography possessor, while *Comprehensive Drug Testing, Inc.* threatened the privacy rights of professional baseball players, a considerably less despised group. At least one commentator has noted the danger posed by the fact most digital search cases result from child pornography prosecutions. RayMing Chang, Note, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 61 (2007). In theory, this may lead courts to adopt more permissive search standards than they would otherwise. *Id.* This is roughly analogous to the weakening of the Fourth Amendment caused by the War on Drugs, due to the relative unpopularity of the defendants in those cases. See Thomas Regnier, *The “Loyal Foot Soldier”: Can the Fourth Amendment Survive the Court’s War on Drugs?*, 72 UMKC L. REV. 631 (2004).

<sup>125</sup> See Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193 (2005) (arguing that computers are not sufficiently different from conventional document containers to require new protocols); Jekot, *supra* note 94 (exploring alternatives, but not advocating any particular one); Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005) (arguing for abolition of digital plain view on pragmatic grounds); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75 (1994) (arguing for search restrictions based on file formats); Chang, *supra* note 124 (arguing for abolition of plain view in digital searches); David J. S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841 (2005) (arguing that traditional document search rules should apply to digital searches); Recent Case, *supra* note 40 (arguing that plain view should be applicable to digital documents, but only when the particular file containing the incriminating data was responsive to the warrant). Although digital searches have attracted significant scholarly

had some influence on the courts. In its *Carey* decision, the Tenth Circuit cited a *Harvard Journal of Law & Technology* article by Professor Raphael Winick in support of its file-format based search parameter.<sup>126</sup> Professor Winick recommended that the *Tamura* procedure be extended into digital searches in order to preserve the particularity requirements of the Fourth Amendment.<sup>127</sup> The article argued that analogizing computers to physical “containers” and applying “container” precedents was inappropriate to address the Fourth Amendment concerns raised by digital searches.<sup>128</sup> Finally, the article suggested that the government must face a heavy burden in demonstrating probable cause of deception when seeking to conduct a search that does not rely on file names and formats.<sup>129</sup>

Although Professor Winick’s article did not specifically address plain view in the context of digital searches, later articles called for its abolition. Many of them also strongly disagreed with *Carey* and Professor Winick.<sup>130</sup> Those advocating for the abolition of the plain view doctrine based their arguments on several grounds. One argument is that digital plain view, due to its incentivizing of invasive and aimless searches, constitutes a de facto authorization of constitutionally impermissible “general warrants.”<sup>131</sup> This school of thought regards computers as a special and unique situation, comparable to a “tape recorder . . . that’s recording our every thought and every word.”<sup>132</sup>

Professor Orin Kerr has also argued for the abolition of plain view in digital searches, on the ground that this is a more pragmatic approach.<sup>133</sup> He argues that abolishing plain view is not only the least complicated approach to rethinking the plain view doctrine, it is also the most

---

attention, this Comment is the first to advocate a flexible process of search warrant negotiations centered around creating a balance between the privacy costs of the search and the societal interests in punishing a particular crime. *See infra* Part V.

<sup>126</sup> *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (citing Winick, *supra* note 125).

<sup>127</sup> Winick, *supra* note 125, at 108–09 (“A vague allegation that the nature of computer storage somehow requires a full text review of all files in all situations should not be permitted to eviscerate the Fourth Amendment’s particularity requirement.”).

<sup>128</sup> *Id.* at 110.

<sup>129</sup> *Id.* at 108.

<sup>130</sup> *See, e.g.*, Chang, *supra* note 124, at 50 (calling the *Carey* format-based approach to warrant restriction “illusory”); Ziff, *supra* note 125, at 853 (“The *Carey*-Winick approach fails to apply the plain view doctrine to searches of computer files and incorrectly relies on the subjective intent of the searching officer to determine the constitutional limits on the scope of a computer search.”).

<sup>131</sup> Chang, *supra* note 124, at 66.

<sup>132</sup> *Id.* at 67 (internal quotes omitted).

<sup>133</sup> Kerr, *supra* note 125, at 534.

balanced.<sup>134</sup> In the process of removing their ability to claim plain view justifications, it frees law enforcement officers to conduct computer searches in whatever manner they find to be the most efficient way to discover the files particularized in the warrant.<sup>135</sup> Professor Kerr does however admit that this is an “imperfect” approach.<sup>136</sup>

Other articles advocate for continued application of plain view to digital searches. An excellent student note by J.S. Ziff calls for an alternate approach to that recommended by the *Carey-Winick* approach.<sup>137</sup> Ziff argues that the existing limitations of plain view doctrine are sufficient to maintain Fourth Amendment rights in a digital age. Those rights, as defined in *Horton* are: (1) that the officer lawfully be in a position from which to view the object seized in plain view, (2) that the object’s incriminating character be immediately apparent, and (3) that the officer have a lawful right of access to the object itself.<sup>138</sup> Of these requirements, Ziff believes the “immediately apparent” requirement is especially restrictive, since it requires that the government prove it had probable cause to believe that the evidence found in plain view was contraband or evidence of a crime.<sup>139</sup> For these reasons, Ziff concludes that the plain view doctrine can be fairly applied to digital searches.

Thus, the scholarly approaches seem to gravitate toward extremes, calling either for the outright abolition of digital plain view or its unmodified preservation. To some degree, this is because there is no obvious middle ground; either immediately incriminating evidence not described in a search warrant is admissible, or it is not. However, this failure to create a middle ground results in a failure to produce an optimal approach to balancing privacy with the social need for effective criminal investigations. This Comment argues that such a middle ground exists, as described below.

#### V. REBALANCING *COMPREHENSIVE DRUG TESTING, INC.*

*Comprehensive Drug Testing, Inc.* ultimately is an overreaction sparked by the concern that the government has found a major loophole

---

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

<sup>135</sup> *Id.* at 583–84.

<sup>136</sup> *Id.*

<sup>137</sup> Ziff, *supra* note 125; *see also* Clancy, *supra* note 125, at 195 (arguing that digital media should be treated in the same manner as physical containers, such as filing cabinets).

<sup>138</sup> *Horton v. California*, 496 U.S. 128, 134 (1990).

<sup>139</sup> Ziff, *supra* note 125, at 866.

with respect to digital plain view.<sup>140</sup> The en banc panel was concerned that by combining the plain view doctrine with the seemingly arbitrary nature of a digital search, the government will be able to circumvent the Fourth Amendment's prohibition on general searches.<sup>141</sup> However, in creating a judicially-imposed process applicable to all "normal[]" digital search cases, regardless of individual circumstances, the Ninth Circuit has constructed an inefficient solution to a problem that demands a careful approach.<sup>142</sup> Further, by overextending Fourth Amendment protections in this area, the Ninth Circuit risks providing itself, or other courts, with an excuse for not extending them far enough in more deserving locations.<sup>143</sup>

Rather than affixing per se rules, the most adaptable and efficient approach to protecting Fourth Amendment rights in an era of digital searches is to focus, on a case-by-case basis, on the reasonableness of the search.<sup>144</sup> Magistrate judges should deny search warrants which will cause unreasonable harm to legitimate privacy interests, in light of the severity of the crime being investigated and the strength of the probable cause shown. In turn, the government can re-apply and offer search procedures calculated to decrease the privacy costs of their search (as determined by the magistrate). This will help ensure that the social harm caused by government intrusions can be minimized, while allowing the government to narrowly tailor its searches in a manner that minimizes inefficiency.<sup>145</sup>

---

<sup>140</sup> See *CDT II*, 579 F.3d 989, 999 (9th Cir. 2009) ("The sequence of events supports the suspicion that representations in the warrant about the necessity for broad authority to seize materials were designed to give the government access to the full list of professional baseball players and their confidential drug testing records.").

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

<sup>142</sup> *Id.* at 1000. This Comment does not argue that the en banc decision to dismiss the Government's appeal of the "Mahan Order" as untimely was incorrect. Nor does it take issue with the fifth holding of the case, related to return of documents, which seems to reflect the existing interpretation of Fed R. Crim. Pro. 41(g) and addresses concerns regarding government stockpiling of private information. See DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 166–67 (2004).

<sup>143</sup> Cf. Stephanie M. Stern, *The Inviolable Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 101, 116–17 (2010) (arguing that the Supreme Court's absolutist approach to protecting houses under the Fourth Amendment has been used as a justification for denial of Fourth Amendment protections in other contexts).

<sup>144</sup> Cf. *Coolidge v. New Hampshire*, 403 U.S. 443, 509–10 (1970) (Black, J., concurring) ("The test of reasonableness cannot be fixed by per se rules; each case must be decided on its own facts."); see also *United States v. Hill*, 322 F. Supp. 2d 1081, 1088 ("As always under the Fourth Amendment, the standard is reasonableness.").

<sup>145</sup> Alexander A. Reinert notes that often the Court often views privacy costs as those borne by the individual, even though there is a general "collective value" in limiting the number and intrusiveness of government searches. Alexander A. Reinert, *Public Interest(s) and Fourth Amendment Enforcement*, 104 ILL. L. REV. 1461, 1464–65 (2010). This



Furthermore, it is important to remember that, if digital searches are properly monitored and subjected to scrutiny during trial, the digital plain view approach is actually of limited use to the government. This makes the development of extraordinary procedures to limit its abuse unnecessary.

#### A. REASONABLE DIGITAL SEARCHES

In order to obtain a search warrant, the government must demonstrate probable cause to justify their search.<sup>146</sup> Probable cause is an ambiguous phrase, and, historically, the Supreme Court's treatment of it has been somewhat inconsistent. The Court has offered different explanations of what constitutes probable cause throughout its history.<sup>147</sup> It remains unclear whether or not probable cause even means that a certain suspicion must be more likely than not to be valid.<sup>148</sup> Professor Craig Lerner, among others, has raised the question of whether probable cause is, in fact, not a fixed probability, but is rather variable, depending on the overall "reasonableness" of a particular search requested by the government.<sup>149</sup> Professor Lerner explains that "reasonableness" can be explained in a

---

Comment similarly refers to such costs as "social costs" rather than purely individual ones, although individual costs can typically be calculated in a more direct and intuitive manner than broader social costs.

<sup>146</sup> U.S. CONST. amend. IV; *United States v. Knights*, 534 U.S. 112, 121 (2001) (stating that "the Fourth Amendment ordinarily requires the degree of probability embodied in the term 'probable cause'").

<sup>147</sup> *Compare* *United States v. Locke*, 11 U.S. (7 Cranch) 339, 348 (1813) (Marshall, C.J.) ("[Probable cause] imports a seizure made under circumstances which warrant suspicion."), *with* *United States v. Carroll*, 267 U.S. 132, 161 (1924) (Taft, C.J.) (defining probable cause as a "reasonable ground for belief of guilt"), *and* *United States v. Brinegar*, 338 U.S. 160, 175 (1949) (noting that probable cause requires "less than evidence which would justify . . . conviction" but "more than mere suspicion"), *and* *Texas v. Brown*, 460 U.S. 730, 742 (1983). *See generally* Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951, 979-90 (2003) (providing a history of the Supreme Court's attempts to define probable cause).

<sup>148</sup> *See* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 3.2(e) (4th ed. 2004) (reviewing a trio of modern Supreme Court cases and concluding that they do not expressly answer the question of whether probable cause means more-probable-than-not); *see also* Lerner, *supra* note 147, at 996 ("[T]he Court's statement that probable cause is more than a suspicion and less than beyond a reasonable doubt places it somewhere between .01% and 90%, which, when all is said and done, is not all that helpful.").

<sup>149</sup> Lerner, *supra* note 147, at 951 ("The reality experienced by American citizens today is that they are searched and seized on a regular basis, and for the vast majority of these searches (e.g., airport searches, street stops, DUI checkpoints, urine testing of government employees), the constitutionality seems to turn not on probable cause, but on the reasonableness of the search, factoring in the degree of the intrusion and the gravity of the investigated offense."); *see also* Joseph D. Grano, *Probable Cause and Common Sense: A Reply to the Critics of Illinois v. Gates*, 17 U. MICH. J.L. REFORM 465, 474 (1984).

search and seizure context using a modified version of the Hand Formula—a tool famous for estimating “reasonableness” in the context of negligence.<sup>150</sup>

The Hand Formula, as displayed below, seeks to optimize the balance between preventing unintentional harms and the expenses of such precautions:<sup>151</sup>

$$B < P \times L$$

Negligence can be inferred when the costs of taking action to prevent an accident ( $B$ ) are less than the product of the costs of the harm caused by the accident ( $L$ ) and the probability of the accident occurring ( $P$ ).

Similarly, Professor Lerner creates a version modified for use in evaluating the reasonableness of searches under the Fourth Amendment:<sup>152</sup>

$$C < V \times P$$

Here, a search is reasonable if the costs of the privacy invasion ( $C$ ) are less than the product of the social benefit of obtaining evidence of a particular crime ( $V$ ) and the probability of such evidence being found in a particular place ( $P$ ).<sup>153</sup> Professor Lerner provides an example of how this might work:

[A]ssume that there is a twenty percent chance that police will uncover evidence of tax fraud among a suspect’s personal papers in his home. The social benefit of a conviction is \$100,000, and the privacy intrusion associated with a search of one’s personal papers is \$50,000. The expected benefit or value of a search would be \$20,000 (\$100,000 x .2), which is less than the expected cost of \$40,000 (\$50,000 x .8). Thus, the search would be unreasonable in these circumstances.<sup>154</sup>

Admittedly, assigning specific values to the variables is somewhat arbitrary and, despite the use of formulae, subjective.<sup>155</sup> This is a simple reality of many multi-factor balancing tests. The value of this approach is

<sup>150</sup> Lerner, *supra* note 147, at 1019–20 (citing *United States v. Carroll Towing*, 159 F.2d 169, 173 (2d Cir. 1947) (Hand, J.)).

<sup>151</sup> RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* § 6.1 (5th ed. 1998).

<sup>152</sup> Lerner, *supra* note 147, at 1019–20. This formula is hereinafter referred to as the “Lerner Formula.”

<sup>153</sup> *Id.* Professor Lerner presents an additional formula:  $P \times V > (1-P) \times C$ , in an attempt to incorporate Supreme Court holdings stating that no invasion of privacy occurs when the government seizes contraband. *See, e.g., United States v. Place*, 462 U.S. 696, 707 (1983). He further modifies the formula to incorporate a “privacy multiplier” called  $m$  to reflect the fact that the harm caused by a search may vary depending on context. This produces the formula:  $P \times V > (1-P) \times (C \times m)$ . For the sake of simplicity, this Comment focuses on the first iteration of the formula.

<sup>154</sup> Lerner, *supra* note 147, at 1020.

<sup>155</sup> *Id.*

primarily heuristic, and its role is not to ensure perfect cost-benefit analysis of search warrant applications, but to ensure that magistrate judges consider both the costs of invasions of privacy and the social costs of undeterred crime when determining whether or not a search is reasonable. Furthermore, by having a simple and understandable framework, they can more easily coordinate their efforts with other magistrates and can more easily incorporate guidance from their appellate courts.<sup>156</sup>

Although this approach has faced criticism,<sup>157</sup> this balancing of privacy and social interests can be found in existing Supreme Court jurisprudence.<sup>158</sup> For instance, in *Winston v. Lee*, the Supreme Court reviewed a restraining order brought by an armed robbery suspect to prevent the Commonwealth of Virginia from removing a bullet from the deep muscle tissue of his chest.<sup>159</sup> The police believed the bullet would prove that the man had been shot while attempting to rob a store.<sup>160</sup> The operation to remove the bullet would require the use of a general anesthetic

---

<sup>156</sup> See Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach*, 97 J. CRIM. L. & CRIMINOLOGY 477, 477 (2007) (arguing for a quantitative “economically-informed” approach to assessing the reasonable expectations of privacy regarding novel technologies instead of the more indeterminate “moral” approach to privacy). Cf. Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978) (assessing the value of privacy in the context of torts in commercial and personal contexts).

<sup>157</sup> See LAFAVE, *supra* note 148, at § 3.2(a) (“The problem with the balancing approach . . . is that it converts the fourth amendment into one immense Rorschach blot. The varieties of police behavior and of the occasions that call it forth are so innumerable that their reflection in a general sliding scale approach could only produce more slide than scale.”); Kit Kinports, *Commentary: Diminishing Probable Cause and Minimalist Searches*, 6 OHIO ST. J. CRIM. L. 649, 655 (2009) (disputing Professor Lerner’s interpretation of case law).

<sup>158</sup> *Brinegar v. United States*, 338 U.S. 160, 183 (1949) (Jackson, J. dissenting) (“[I]f we are to make judicial exceptions to the Fourth Amendment for these reasons, it seems to me they should depend somewhat upon the gravity of the offense.”); see also *Maryland v. Buie*, 494 U.S. 325, 331 (1990) (“[I]n determining reasonableness, we have balanced the intrusion on the individual’s Fourth Amendment interests against its promotion of legitimate governmental interests.”); *Hudson v. Palmer*, 468 U.S. 517, 527 (1984) (“Determining whether an expectation of privacy is “legitimate” or “reasonable” necessarily entails a balancing of interests.”); *Terry v. Ohio*, 392 U.S. 1, 8, 21–22 (1968) (applying a balancing test to assess the reasonableness of an officer’s “pat-down” search); *Camara v. Municipal Court of San Francisco*, 387 U.S. 523, 536–37 (1967) (“Unfortunately, there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails.”). *But see Dunaway v. New York*, 442 U.S. 200, 208 (1979) (rejecting the notion that privacy and governmental interests must be balanced on a case-by-case basis).

<sup>159</sup> 470 U.S. 753, 757 (1985).

<sup>160</sup> *Id.* at 755–56. The suspect claimed that he had been shot while being mugged. *Id.* at 756.

and could have taken anywhere between twenty minutes and two-and-a-half hours to complete.<sup>161</sup> As with any surgery, the procedure carried risks of complications, infection, or over-anesthetization.<sup>162</sup>

The Court held that the reasonableness of surgical intrusions beneath the skin depends on a case-by-case approach, in “which the individual’s interests in privacy and security are weighed against society’s interests in conducting the procedure.”<sup>163</sup> The Court found that the surgical procedure, although justified by probable cause, constituted an extreme intrusion into the bodily integrity and personal privacy of the suspect.<sup>164</sup> It noted that such a serious intrusion easily outbalanced the Commonwealth’s need to retrieve the bullet, since other evidence could be used to establish the connection between the suspect and the robbery (such as identification by the storekeeper who shot him, and the fact that the suspect was found eight blocks away from the store only twenty minutes after the robbery.)<sup>165</sup> The Court contrasted the circumstances of compelled surgery against the security of “houses, papers, and effects.”<sup>166</sup>

*Winston* clearly demonstrates a process of balancing in reviewing police actions for compliance with the Fourth Amendment. The case would have clearly been resolved differently if the bullet had been lodged in the defendant’s shoe instead of his chest. The Court hints that the case may have been decided in a different manner if the bullet had been essential to the case, rather than relatively disposable. The case also shows, not only that the amount of probable cause necessary to justify warrants varies depending on the circumstances, but that sometimes even a high degree of probable cause cannot justify an unnecessary search with high privacy costs. *Winston* reflects an effective illustration of why flexibility, rather than per se rules, can sometimes be the only way to maintain Fourth Amendment protections in novel situations, such as digital searches.

---

<sup>161</sup> *Id.* at 764.

<sup>162</sup> *Id.* In its earlier decision, the court of appeals deemed these risks “minimal”. *Id.* at 764 n.7. The Supreme Court ultimately concluded that the actual risks of harm were “apparently not severe” but were at least “a subject of considerable dispute” and “uncertain[.]” *Id.* at 766.

<sup>163</sup> *Id.*

<sup>164</sup> *Id.* at 765.

<sup>165</sup> *Id.* at 756, 765 (noting that the suspect was identified by the storekeeper who had shot him, and the suspect had been found shot eight blocks away from the store only twenty minutes after the storekeeper shot the man robbing him).

<sup>166</sup> *Id.* at 759 (quoting U.S. CONST. amend. IV).

## B. APPLYING THE LERNER FORMULA TO DIGITAL SEARCHES

The Lerner Formula presents an adaptable and practical approach for reconciling the need for digital searches with the Fourth Amendment and rising expectations of privacy in digital storage media. The privacy costs of a file-by-file digital search vary by computer, but it can generally be assumed to be fairly high. The privacy costs of searching a computer used almost exclusively for criminal purposes are probably low, because the files particularized in the warrant are intermingled with a relatively small number of non-particularized files. However, most computers targeted for search are personal computers.<sup>167</sup> Personal computers play an increasingly central role in modern life and they often contain correspondence, personal records, medical information, and other forms of private information.<sup>168</sup> A file-by-file search of these records would carry serious privacy costs, although perhaps less severe than the privacy costs of the compelled surgery at issue in *Winston*.<sup>169</sup> If a computer is owned or shared by people who are not under suspicion, the privacy costs would typically increase further.<sup>170</sup>

However, these privacy costs will not always outweigh society's need to investigate crimes. Searches of "persons, houses, papers, and effects" can be justified when the public need for evidence rises to a sufficient level.<sup>171</sup> Courts regularly permit searches of homes and personal records,<sup>172</sup> despite the high privacy expected in those areas.<sup>173</sup>

Furthermore, digital searches create less of a practical intrusion than searches of intermingled paper documents, like the search in *Tamura*.<sup>174</sup>

---

<sup>167</sup> See generally cases summarized *supra* Part IV.

<sup>168</sup> Kerr, *supra* note 125, at 532.

<sup>169</sup> *Winston*, 470 U.S. at 753.

<sup>170</sup> *Trulock v. Freeh*, 275 F.3d 391, 403–04 (4th Cir. 2001).

<sup>171</sup> *Winston*, 470 U.S. at 759.

<sup>172</sup> See, e.g., *United States v. Williams*, 592 F.3d 511, 521–25 (4th Cir. 2010) (permitting plain view discovery of gun in locked case during search of any container within a suspect's house large enough to contain a data storage device); *United States v. Reyerson*, No. 3:09-CR-66, 2010 U.S. Dist. LEXIS 21237, at \*9 (E.D. Tenn. Feb. 12, 2010) (upholding removal of cabinet during search of mobile home for drugs).

<sup>173</sup> See *U.S. v. Karo*, 468 U.S. 705, 714 (1984) ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant . . ."); see also *Dow Chem. Co. v. United States*, 476 U.S. 227, 237 n.4 (1986) ("We find it important that this is not an area immediately adjacent to a private home, where privacy expectations are most heightened.").

<sup>174</sup> In fact, the *Tamura* decision cites a prior decision in which investigators were allowed to conduct an intermingled documents search without the supervision of a neutral magistrate when their search could be conducted on-site and would not require a seizure. *United States v. Tamura*, 694 F.2d 591, 596 n.4 (citing *Forro Precision, Inc. v. IBM Corp.*, 673 F.2d 1045,

Large-scale document seizures have heightened privacy costs, because they deprive the owners of those documents the ability to access them while the search is conducted and require the prolonged presence of government agents on the owner's property.<sup>175</sup> By contrast, when conducting a digital search, government agents can, upon a showing of necessity to the magistrate, create a "bitstream copy" of the records.<sup>176</sup> A bitstream copy is an exact reproduction of a digital record, and includes all data within the record, including hidden or even "deleted" files.<sup>177</sup> The target of the warrant is able to keep their records, while the government is then able to execute the search warrant without causing undue interference. Thus, the limited practical intrusion of digital searches may play an important role in a magistrate's calculation of privacy costs in some cases.

When applying the Lerner Formula, magistrates must also weigh the public necessity of conducting a particular digital search. One factor of central importance is the social cost of the crime being investigated, which will vary by case.<sup>178</sup> However, magistrates should also take into account

---

1053–54 (9th Cir. 1982) and distinguishing the case as involving a search, rather than a seizure).

<sup>175</sup> For a particularly egregious example, see *Steve Jackson Games, Inc. v. United States Secret Service*, 816 F. Supp. 432, 437 (W.D. Tex. 1993) (owner of electronic bulletin board had computers and disks seized; court found no valid reason why information sought could not be copied and equipment returned within hours), *aff'd* 36 F.3d 457 (5th Cir. 1994).

<sup>176</sup> *United States v. Hunter*, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) ("At the very least, the government should copy and return the equipment as soon as possible.").

<sup>177</sup> Kerr, *supra* note 125, at 541. A bitstream copy may contain deleted files because most computer hard drives, when directed to delete information, do not actually wipe the sectors of the hard drive containing that information clean. Rather, they mark those sectors as a suitable location to overwrite with new data. However, until that new data arrives, the "deleted" data remains in that location. See Craig Ball, *Computer Forensics for Lawyers Who Can't Set the Clock on Their VCR*, in 6 ON FORENSICS 29–30 (2005), available at [http://www.craigball.com/cf\\_vcr.pdf](http://www.craigball.com/cf_vcr.pdf).

<sup>178</sup> Professor Lerner's article recognizes that varying probable cause requirements depending on the severity of the crime alleged is a "minority view" suggested by Justice Jackson's dissent in *United States v. Brinegar*, 338 U.S. 160, 180–82 (1949) and *Camara v. Municipal Court of San Francisco*, 387 U.S. 523, 536–37 (1967). Lerner, *supra* note 147, at 1015–19. Justice Jackson's view has found some support from leading jurists, including Judge Friendly and Judge Posner. See *United States v. Soyka*, 394 F.2d 443, 452 (2d Cir. 1968) (Friendly, J. dissenting) ("If [the] decision were mine to make, I would not be at all averse to straightforward recognition that the gravity of the suspected crime and the utility of the police action . . . are factors bearing on the validity of the search or arrest decision."); *Llaguno v. Mingey*, 763 F.2d 1560, 1566 (7th Cir. 1984) (en banc) (Posner, J.) ("The amount of information that prudent police will collect before deciding to make a search or an arrest, and hence the amount of probable cause they will have, is a function of the gravity of the crime, and especially the danger of its imminent repetition."). Ultimately the question of whether or not it is appropriate to consider the severity of the alleged crime is a subject of considerable debate. See Kerr, *supra* note 125, at 581 (describing the practice of varying

the general need for the government to effectively detect and investigate crime in a digital age. The increased availability of computing power and telecommunications has created new forms of crime and has made many existing crimes easier to commit.<sup>179</sup> It also makes evidence of crime more difficult to detect or investigate due to the likelihood of mislabeling,<sup>180</sup> or disguise,<sup>181</sup> the exponentially increasing size of databases,<sup>182</sup> and the widespread availability of encryption technology.<sup>183</sup> Digital crime also

---

permissible search procedures based on severity of offense “problematic”); Eugene Volokh, *Crime Severity and Constitutional Line-Drawing*, 90 VA. L. REV. 1957, 1983 (2004) (“We may all agree that there is a difference between murder and littering, but it doesn’t follow that courts can create administrable lines that distinguish the various cases between the two extremes.”). *But see* Jeffrey Bellin, *Crime Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World* 38–41 (S. Methodist Univ., Working Paper No. 64, 2010), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1692312](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1692312) (arguing that considering crime severity may help limit the potential for new technologies to allow for particularly intrusive searches). Ultimately, this question is not a focus of this Comment, which instead will focus on the public interest in conducting efficient digital investigations regardless of the crime investigated.

<sup>179</sup> See Robin Bryant, *The Challenge of Digital Crime*, in INVESTIGATING DIGITAL CRIME 1–11 (Robin Bryant, ed. 2008) (listing the inherent advantages of digital crimes, including spatial and temporal benefits, economies of scale, anonymity, “legislative lag,” and improved concealment); see also James J. Tomkovicz, *The Effect of Technology on Fourth Amendment Analysis and Individual Rights*, 72 MISS. L.J. 317, 319 n.5 (2002) (collecting examples of computer crimes). See generally *Privacy and Cybercrime Enforcement, Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 110th Cong. (2007) (statement of Andrew Lourie, Acting Principal Deputy Assistant Att’y Gen. and Chief of Staff Criminal Division, U.S. Department of Justice).

<sup>180</sup> See *United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, at \*36 (S.D.N.Y. Apr. 4, 2007) (“[I]t is precisely because computer files can be intermingled and encrypted that the computer is a useful criminal tool.”). See generally Ross E. Mayfield, *Investigative Strategy and Utilities*, in FORENSIC COMPUTER CRIME INVESTIGATION 105 (Thomas A. Johnson, ed., 2006).

<sup>181</sup> See Whitson Gordon, *Hide Secret Files in Office 2007 Documents*, LIFEHACKER (May 13, 2010), <http://lifehacker.com/5538370/hide-secret-files-in-office-2007-documents>.

<sup>182</sup> See Ziff, *supra* note 125, at 860–61 (noting the exponential growth of digital databases and the increasing impracticality of the approaches advocated in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982) and Winick, *supra* note 125); see also PETER GRABOWSKY, *ELECTRONIC CRIME* 70 (2d ed., 2007) (“[T]he metaphor of the needle in the haystack is not entirely inappropriate. Even with automated search tools, finding that needle may be extremely difficult and time-consuming.”).

<sup>183</sup> See, e.g., *United States v. Kim*, 677 F. Supp. 2d 930, 934 (S.D. Tex. 2009) (noting that investigators required two months to decode encrypted files); EOGAN CASEY, *DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET* 498 (2d ed. 2004) (describing investigator difficulty in detecting activities of online child pornography distribution ring due to encryption). In some cases, the very act of shutting down and seizing computer hardware can result in the permanent loss of encrypted data. NAT’L INST. OF JUSTICE, *INVESTIGATIVE USES OF TECHNOLOGY: DEVICES, TOOLS, AND TECHNIQUES* 51 (2007), available at <http://www.ncjrs.gov/pdffiles1/nij/213030.pdf>.

creates a sense of distance and anonymity that may encourage those likely to be deterred from committing conventional crimes to commit digital ones.<sup>184</sup> Society has an interest in detecting both digital crimes and traditional crimes that now create digital evidence. If courts fail to take these interests into account, they risk making an already complicated and difficult form of investigation even more so.

Ultimately, the greatest advantage of establishing this system of balances is the efficient negotiation that can be encouraged by magistrates. If a magistrate rejects a search warrant application after finding that it carries an unduly high privacy cost, then an investigator responding to this decision must attempt to change the variables in the Lerner formula if she still wants to obtain a search warrant. However, she typically cannot change the magistrate's assessment of the search's social costs. And while improving the probability variable is possible in some cases, this will be impossible in many cases, especially if the investigation requires a digital search to proceed any further. Therefore, the investigator will most often be forced to offer compromises in order to reduce the privacy costs.

These compromises will produce much more efficient results than the judicially-imposed processes contemplated in *Comprehensive Drug Testing, Inc.* Investigators will have their choice of what concessions to offer, and can suggest compromises that minimize impairment of the investigation while offering a sufficient reduction in privacy cost to obtain the approval of the magistrate. For instance, in some cases investigators may have enough information about the target computer and the targeted files to develop a search protocol designed to minimize the amount of non-pertinent material that comes into view. In other cases, investigators may know little about the file systems of the target system and may have reason

---

Additionally, federal officials recently discovered a Russian spy ring that communicated, in part, by using commonly-available steganography programs to hide communications in innocuous-looking image files. Stuart Fox, *How Russian Spies Hid Secret Codes in Online Photos*, CSMONITOR.COM (June 30, 2010), <http://www.csmonitor.com/Science/2010/0630/How-Russian-spies-hid-secret-codes-in-online-photos>. The investigators discovered the hidden messages, not through sophisticated electronic surveillance, but by searching the homes of the spies and finding the password necessary to decrypt the messages written on a piece of paper next to a computer. Noah Shachtman, *FBI: Spies Hid Secret Messages on Public Websites*, WIRED (June 29, 2010), <http://www.wired.com/dangerroom/2010/06/alleged-spies-hid-secret-messages-on-public-websites>.

<sup>184</sup> See Susan W. Brenner, *Is There Such A Thing As "Virtual Crime"?*, 4 CAL. CRIM. LAW REV. 1, ¶125; Monique Mattei Ferraro & Joseph Sudol, *Internet Crimes Against Children*, in FORENSIC COMPUTER CRIME INVESTIGATION 129, 131 (Thomas A. Johnson ed., 2006).



to believe that the computer's owner has mislabeled or disguised files.<sup>185</sup> Under these circumstances, rather than offering a search protocol to the magistrate, the investigators may suggest other concessions.<sup>186</sup>

The en banc *Comprehensive Drug Testing, Inc.* decision helpfully suggests what kinds of concessions they could make. They could waive plain view for all documents that are not responsive to the warrant,<sup>187</sup> or simply waive it entirely.<sup>188</sup> They could have the search conducted by technicians under the supervision of a magistrate.<sup>189</sup> In circumstances where the digital databases belong to a third party not suspected of wrongdoing, the government could agree to conduct their search in collaboration with the database owner.<sup>190</sup> If the contents of the file being searched for are already known, which can occur in some cases, the

---

<sup>185</sup> Michael G. Noblett, Mark M. Pollitt, & Lawrence A. Presley, *Recovering and Examining Computer Forensic Evidence*, 2 FORENSIC SCIENCE COMM. 7 (2000), available at [www.fbi.gov/hp/lab/fsc/backissue/oct2000/computer.htm](http://www.fbi.gov/hp/lab/fsc/backissue/oct2000/computer.htm) (observing that there is “no such thing as generic computer science procedures” and that “evidence is likely to be significantly different every time a submission is received by the laboratory and will likely require an examination plan tailored to that particular evidence”).

<sup>186</sup> This process of negotiation renders unnecessary the third holding of *Comprehensive Drug Testing, Inc.*, which required “disclos[ure of the] actual risks of destruction of information.” See *CDT II*, 579 F.3d 989, 1006 (9th Cir. 2009). Demanding that agents determine “actual risks of destruction,” is a requirement that is as daunting to agents as it is difficult for magistrates to enforce. The negotiation process is a more effective way of ensuring that agents develop honest estimates of risk of destruction or disguise. Agents must develop fair estimates of these risks, otherwise they will offer search concessions that make their search unnecessarily difficult.

<sup>187</sup> Recent Case, *supra* note 40, at 1009–10 (dubbing this the “responsive document approach”).

<sup>188</sup> *CDT II*, 579 F.3d at 997–98, 1006. The degree to which waiver of plain view actually reduces privacy costs is something of an open question. The knowledge that investigators may not use digital evidence against a target if that evidence was discovered while searching for evidence of an unrelated crime may decrease privacy concerns to an extent. Nonetheless, they do not reduce the costs entirely, since the private files will still be viewed by government agents (or, under the *Comprehensive Drug Testing, Inc.* approach, government technicians and possibly a supervising magistrate.) The complex nature of privacy complicates these determinations about when privacy rights have been impaired and to what degree they have been impaired. See Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) (categorizing modern privacy interests in four groups: information collection, information processing, information dissemination, and invasion).

<sup>189</sup> *CDT II*, 579 F.3d at 1000–01, 1006.

<sup>190</sup> *CDT* offered some limited assistance to the government in determining where the records of the ten players could be found. *CDT I*, 473 F.3d 915, 922 (9th Cir. 2006).

government could agree to use a hashing program to retrieve the file without viewing any other files in the computer.<sup>191</sup>

This negotiation process will encourage the government to develop efficient search methods that take into account the privacy concerns raised by digital searches while discouraging the existing temptation to claim that a file-by-file search is required in all cases. The process does, however, require that magistrate judges take an active role in scrutinizing warrant applications and ensuring a balance. Magistrates are increasingly familiar with digital searches and have been addressing the issues they pose for over a decade.<sup>192</sup> Although there is reason to expect that not all judges will enforce this system aggressively enough,<sup>193</sup> the benefits are significant, and the appellate courts should attempt to coordinate and guide the magistrate judges as much as is possible.

### C. COMPREHENSIVE DRUG TESTING, INC. AND REASONABLENESS

Due to the heuristic nature of the Lerner Formula, it is difficult to conclusively say whether or not the *Comprehensive Drug Testing, Inc.* holding is incorrect. However, the process used to reach it was undesirable, and it is clearly not an appropriate approach for all digital searches. The government's search of the CDT and Quest records did raise several sources of privacy cost. The records were quasi-medical in nature and belonged to numerous third parties not under immediate suspicion of drug use.<sup>194</sup> If such searches were permitted in the future, it might be impossible for the \$620 million drug testing industry to remain operational due to their inability to guarantee the confidentiality of their test results.<sup>195</sup> The search

---

<sup>191</sup> See, e.g., *United States v. Borowy*, 595 F.3d 1045, 1047–48 (9th Cir. 2010) (suspect is detected sharing particular files using a peer-to-peer file-sharing program and investigators conduct a search of his computer).

<sup>192</sup> *Supra* Part IV.C.

<sup>193</sup> See, e.g., William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 VA. L. REV. 881, 888–89 (1991) (describing the modern warrant process as “slapdash” and “casual”); Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 34 (1988) (calling “the ‘rubber stamp’ quality of magistrate review of warrant applications” an “open scandal”).

<sup>194</sup> On the other hand, Barry Bonds did not believe that his results were confidential, and was concerned that Major League Baseball would leak his results to the media if they felt it necessary to do so. See FAINARU-WADA & WILLIAMS, *supra* note 2, at 127. Nonetheless, all participating players had been promised confidentiality by Major League Baseball and had been told that the purpose of the testing was to see if more than five percent of them tested positive, in which case further screening would be used. *CDT II*, 579 F.3d at 993.

<sup>195</sup> MARKETDATA ENTERPRISES, INC., THE U.S. MEDICAL LABORATORIES INDUSTRY 10 (9th ed. 2007) (on file with the *Journal of Criminal Law & Criminology*).

of CDT and Quest carried what can be assumed to be well above-average privacy costs.

Those privacy costs were not outweighed by the probability variable or the social costs of undetected crime. Although the records were sure to contain drug testing results for the ten players, it is unclear whether or not it was strongly likely that those results would be positive. The Government was investigating BALCO, a company that had specialized in developing undetectable performance-enhancing drugs.<sup>196</sup> Furthermore, as Judge Thomas noted in his dissent in *CDT I*, a positive result would not have been conclusive proof of drug use.<sup>197</sup> Additionally, the crime under investigation was not of a particularly severe nature, and did not immediately threaten human life.<sup>198</sup> Finally, just as the police in *Winston* could have proven the suspect's involvement in an armed robbery without retrieving the bullet, the BALCO investigation could likely have demonstrated the drug use of the targeted players without accessing the CDT databases.<sup>199</sup>

The Ninth Circuit approach does not strike an appropriate balance under the Lerner Formula. Although the above-average privacy costs of the government search in this case require mitigation, it is not at all clear that all of the procedures required by the Ninth Circuit are necessary to restore the balance. Simply requiring the government to develop a search protocol that could be reasonably expected to retrieve only the test results of the targeted players would have been sufficient to reduce the privacy costs to adequate levels. As Judge Bea noted in his partial dissent, the drug test results of the ten players were located within a Microsoft Excel spreadsheet, along with many other baseball players.<sup>200</sup> However, the spreadsheet, when opened, only immediately displayed the names of the players; viewing the test results required investigators to scroll right. Therefore, investigators could have easily adopted a search protocol whereby they would remove the results of the other baseball players before scrolling and viewing the test results.<sup>201</sup> It is therefore difficult to see how the additional procedural

---

<sup>196</sup> See *supra* note 5.

<sup>197</sup> 473 F.3d 915, 945 (9th Cir. 2006) (Thomas, J. dissenting).

<sup>198</sup> In contrast, Justice Jackson's dissent in *United States v. Brinegar* uses the example of a kidnapped child to demonstrate a crime carrying high social costs. 338 U.S. 160, 183 (1949) (Jackson, J. dissenting).

<sup>199</sup> The Government may have been able to use the seized records of BALCO or obtain the cooperation of Victor Conte or other intermediaries to establish the use of performance-enhancing drugs by the ten players. FAINARU-WADA & WILLIAMS, *supra* note 2.

<sup>200</sup> *CDT II*, 579 F.3d 989, 1016 & n.2 (9th Cir. 2009).

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

requirements advanced by the Ninth Circuit would produce anything more than marginal reductions in privacy cost.<sup>202</sup>

And while the redundancy of the Ninth Circuit procedures creates marginal benefits, they risk making all digital searches significantly more difficult and expensive to conduct.<sup>203</sup> For instance, the requirement that only specialized personnel be allowed to perform file segregation is unrealistic and expensive if applied to every digital search.<sup>204</sup> To properly segregate pertinent files from non-pertinent files typically requires detailed knowledge of the investigation.<sup>205</sup> This is especially true in the execution

---

<sup>202</sup> The Ninth Circuit's minimization procedures resemble (and probably exceed) the procedures regulating searches of records intermingled with documents protected by attorney-client privilege. These procedures include the use of "taint teams" or requiring searches to be conducted by magistrates *in camera*. See, e.g., Klitzman, Klitzman and Gallagher v. Krut, 744 F.2d 955, 962 (3d Cir. 1984) (discussing the use of a special master to review documents seized from a law firm in camera); United States v. Skeddle, 989 F. Supp. 890, 905 (N.D. Ohio 1997) (upholding segregation by "taint team"). Searches of records protected by attorney-client privilege carry extremely high privacy costs since they threaten to undermine constitutional rights to counsel. Although the search of CDT's drug records raise serious privacy concerns, it is difficult to see how the Ninth Circuit could conclude that the privacy costs were so high that search minimization procedures equal to or perhaps greater than those granted to searches of attorney-client communications were necessary. For an excellent discussion of searches of documents containing intermingled privileged documents, see Eric D. McArthur, Comment, *The Search and Seizure of Privileged Attorney-Client Communications*, 72 U. CHI. L. REV. 729, 732 (2005) (comparing the privacy costs of searches of privileged documents to the compulsory surgery in *Winston v. Lee*, 470 U.S. 753 (1985)).

<sup>203</sup> The holding requiring the destruction of non-pertinent data, inasmuch as it applies to data not otherwise retainable under plain view, is uncontroversial. *CDT II*, 579 F.3d at 1000-01. This seems clear under Fed. R. Crim. P. 41(g) and implicit in Fourth Amendment jurisprudence, given the lack of any legitimate governmental interest in retaining information unlawfully obtained and therefore "poisonous" to the investigation if utilized. *Wong Sun v. United States*, 371 U.S. 471, 485-86 (1963).

<sup>204</sup> *CDT II*, 579 F.3d at 1000; see *id.* at 1013 (Callahan, J. concurring in part, dissenting in part) ("To comply, an agency would have to expand its personnel, likely at a significant cost, to include both computer specialists who could segregate data and forensic computer specialists who could assist in the subsequent investigation. The alternative would be to use an independent third party consultant, which no doubt carries its own significant expense.").

<sup>205</sup> See EOGHAN CASEY DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET 90 (2d ed. 2004) ("[T]he success of [the investigative] process depends heavily on the experience and skill of the investigators, evidence examiners and crime scene technicians who *must collaborate to piece the evidence together* and develop a convincing account of the offense.") (emphasis added); see also *id.* at 101-02, 102 fig.4.5 (listing the steps taken by investigators and examiners "working together" in the course of a digital investigation). See generally ASS'N OF CHIEF POLICE OFFICERS, GOOD PRACTICES GUIDE FOR COMPUTER BASED ELECTRONIC EVIDENCE 24 (2003), available at [http://www.7safe.com/electronic\\_evidence/ACPO\\_guidelines\\_computer\\_evidence.pdf](http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf) (describing the analytical process by which the forensic examiner or other personnel review

of warrants for particular types of evidence, rather than known items or files.

For instance, imagine a search warrant granted by a magistrate to search and seize “hardware, computer disks, [and] disk drives . . . which may be, or are used to visually depict child pornography, child erotica, information pertaining to the sexual interest in child pornography . . . or information pertaining to an interest in child pornography.”<sup>206</sup> An experienced investigator with superior knowledge of the case at hand would be more (perhaps much more) likely to identify “information pertaining to an interest in child pornography” than a technician whose only involvement in the case is to extract and sort information from digital storage media. To insist on such a requirement in all “normal[]”<sup>207</sup> digital search cases is simply unrealistic, which is why no such requirement exists in traditional searches.<sup>208</sup> In failing to evaluate reasonableness through a balancing of social interests and privacy interests, the Ninth Circuit has created an unsustainable system where the ability of the government to conduct efficient investigations arbitrarily depends on whether or not the evidence is digital or non-digital.<sup>209</sup>

#### D. EX ANTE SEARCH RESTRICTIONS

Professor Orin S. Kerr, a leading scholar on the Fourth Amendment implications of digital searches, has recently published an article responding to the *Comprehensive Drug Testing, Inc.* decision.<sup>210</sup> The paper creates two categories of responses to the constitutional questions raised by

---

collects digital information for probative value after it has been retrieved by a forensic examiner).

<sup>206</sup> *United States v. Hall*, 142 F.3d 988 (7th Cir. 1998).

<sup>207</sup> *CDT II*, 579 F.3d at 1000.

<sup>208</sup> For instance, the officers in *Arizona v. Hicks* were not required, after arresting the defendant, to send in “specialized personnel or an independent third party” to search the apartment for weapons or dead bodies. 480 U.S. 321, 326–27 (1987).

<sup>209</sup> See, e.g., *United States v. Williams*, No. 08-5000, 2010 WL 251592, at \*10 (4th Cir. Jan. 21, 2010) (concluding that searches of digital databases are not distinguishable from searches of filing cabinets on the basis of the amount of information inside database); Recent Case, *supra* note 40, at 1010 (“There is no justification for applying different standards to information contained in the same document depending on whether that document is still on a computer or has been printed out.”).

<sup>210</sup> Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010) [hereinafter Kerr, *Ex Ante Regulation*]. In addition to extensive writings on digital searches, cited *supra*, Professor Kerr authored the Department of Justice’s guidelines on digital searches. ORIN S. KERR, *SEARCHING & SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS* (1st ed. 2001), available at <http://permanent.access.gpo.gov/lps11361/searchmanual.pdf>.

digital searches: ex ante restrictions and ex post restrictions. Ex ante restrictions are conditions such as those established by the Ninth Circuit, which dictate to the manner in which the search is to be conducted.<sup>211</sup> Ex post restrictions are court decisions and precedents which limit the admissibility of evidence after the search has occurred.<sup>212</sup> An example would be the review of the actions of the officer in *Hicks* and the finding of noncompliance with the Fourth Amendment based on his moving of the turntable during the search.

Professor Kerr argues that ex post restrictions should be the only tool at the disposal of courts for enforcing Fourth Amendment protections in digital search cases (or, apparently, any kind of government search). First, Professor Kerr argues that magistrate judges lack authority to impose ex ante requirements other than particularity and probable cause.<sup>213</sup> Professor Kerr bases this assessment on a set of Supreme Court cases that, while not specifically addressing the authority of magistrates to establish ex ante restrictions in all cases, would seem to bring it into some doubt. For instance, in the context of anticipatory warrants, the Court has rejected the argument that, in addition to the requirements of probable cause and particularity, there exists a requirement that the circumstances activating the warrant also be particularly described, suggesting that particularity and probable cause may be the only two requirements a magistrate can place on a search warrant.<sup>214</sup> It has also held that magistrates cannot uphold their duties while directly participating in searches as if they were an “adjunct law enforcement officer”<sup>215</sup> and that a warrant for a wiretap does not require additional language authorizing the act of entering the target’s residence to install the surveillance equipment.<sup>216</sup> Additionally, in *Richards v. Wisconsin*, the Court cast doubt on whether or not ex ante restrictions are enforceable at all, when it upheld a search that disregarded an ex ante requirement to “knock and announce” prior to entering a suspect’s hotel room.<sup>217</sup>

---

<sup>211</sup> See Kerr, *Ex Ante Regulation*, *supra* note 210, at 1243–44.

<sup>212</sup> *Id.* at 1261.

<sup>213</sup> *Id.*

<sup>214</sup> See *United States v. Grubbs*, 547 U.S. 90, 97 (2006).

<sup>215</sup> *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 321 (1979). This case involved a magistrate who assisted a search for obscene materials by going to the adult bookstore with the officer, reviewing the obscene material seized there, and informing the searching officers of whether or not the materials met the constitutional requirements for obscenity. *Id.* at 321.

<sup>216</sup> *Dalia v. United States*, 441 U.S. 238 (1979).

<sup>217</sup> 520 U.S. 385 (1997).

Professor Kerr further argues that, regardless of the authority of magistrates to impose enforceable ex ante restrictions, ex ante restrictions are normatively undesirable and should be avoided. Professor Kerr argues that, unlike ex post restrictions, ex ante restrictions tend to limit the ability for appellate courts to aid in the development of law in an area of law that is in need of more clarity as to what is and is not reasonable.<sup>218</sup> The reasonableness determinations required for ex ante restrictions must also be made at a phase of an investigation where only a limited amount of information is available to the magistrate. The number of digital media to be searched, their formatting, the likelihood of encryption, and other variables may not be known until the search is conducted, limiting the accuracy of reasonableness determinations and introducing constitutional error.<sup>219</sup> Professor Kerr concludes that, in the face of these difficulties, ex ante restrictions should be avoided.

Professor Kerr's arguments are provocative and deserve a more thorough review than this Comment can provide. Ex ante search restrictions, while not apparently adopted by the Supreme Court, have been adopted by several courts of appeals<sup>220</sup> and a scattering of district courts.<sup>221</sup> Prohibiting them would result in the reversal of a significant swathe of appellate Fourth Amendment jurisprudence.

Professor Kerr concedes that the Supreme Court has not issued a definitive ruling on whether or not ex ante restrictions are permissible, leaving some room for debate.<sup>222</sup> However, the approach advocated in this Comment circumvents that debate. The ex ante requirements of particularity and probable cause are clearly permitted and this Comment's approach is grounded in probable cause. A magistrate reviewing a search warrant must assure that the probable cause requirement is met, and he cannot know what level of probable cause is required without assessing the overall reasonableness of the search. Magistrates have the authority to deny

---

<sup>218</sup> Kerr, *Ex Ante Regulation*, *supra* note 210, at 1277–78.

<sup>219</sup> *Id.*

<sup>220</sup> The ex ante *Tamura* procedure is still valid precedent in the Ninth Circuit and has received positive appraisals in the Third and Tenth Circuits. See *United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars*, 307 F.3d 137, 154 (3d Cir. 2002); *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999). Similarly, the Third Circuit has advocated ex ante restrictions in the context of searches of law firm documents. See *Klitzman, Klitzman & Gallagher v. Krut*, 744 F.2d 955, 962 (3d Cir. 1984); see also *United States v. Rayburn House Office Building, Room 2113, Washington D.C. 20515*, 497 F.3d 654, 656 (D.C. Cir 2007) (reviewing a government search pursuant to a warrant requiring “special procedures” for the search of a congressman's office).

<sup>221</sup> See *supra* note 119.

<sup>222</sup> Kerr, *Ex Ante Regulation*, *supra* note 210, at 1270.

search warrants where the probable cause requirement is not met. To the extent that the approach advocated in this Comment may result in ex ante restrictions on searches, it is important to note that those restrictions are self-imposed by the officials requesting the warrant, not the magistrate, who simply adjusts the probable cause required based on the reasonableness of the proposed search.

This raises the question of the impact of *Richards v. Wisconsin* on the enforceability of ex ante search restrictions, since that case leaves the issue in some doubt. Further clarification by the Supreme Court may be necessary, but, at present, the case seems distinguishable from most digital search cases. The *Richards v. Wisconsin* case involved a “knock and announce” requirement and rejected its use as an ex ante requirement.<sup>223</sup> The “unannounced” entry occurred immediately after an officer attempted to enter a suspect’s hotel room disguised as hotel staff. The suspect opened the door, noticed other officers in the hallway and slammed the door.<sup>224</sup> At that point, due to the exigent circumstances and immediate potential for destruction of evidence (as implied by the slamming of the door) the reasonableness factors were significantly different than they had been when the magistrate issued the warrant. Thus, the primary failure of the requirement in that case stemmed from the fact that the magistrate purported to evaluate the reasonableness of a particular aspect of a search (the reasonableness of unannounced entry) at a point in time in which the magistrate did not have sufficient information to make such a judgment.

Digital searches are not nearly as volatile. Once the electronic media has been seized, it is fairly immune to destruction (unless the suspect has imposed highly sophisticated countermeasures). The reasonableness factors surrounding the search do not change as much as they do in the circumstances presented in *Richards*. Thus, *Richards* is more clearly understood as a limit on arbitrary or unsupported ex ante requirements, not all ex ante requirements.

Beyond the question of inherent constitutional authority, there seems to be some authorization in the Federal Rules of Criminal Procedure for ex ante restrictions in the context of digital searches. Rule 41(e)(2)(B) was specifically created by a 2009 amendment to provide additional direction on warrants for electronically stored information.<sup>225</sup> The rule notes that

---

<sup>223</sup> 520 U.S. 385, 388 (1996).

<sup>224</sup> *Id.*

<sup>225</sup> The rule provides:

A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for



although officers only need one warrant in order to both seize or copy electronic media and then review that material, that is only the default rule. If the magistrate “otherwise specific[s]” then the default does not apply, meaning that a magistrate can authorize the initial seizure, but stay the review of the material.<sup>226</sup>

In an ex post-only system, this carve out would make little sense. If the probable cause and particularity requirements justified the seizure, then there would be no justification for delaying a review of the seized material. Rather, this “otherwise specified” clause seems to provide for magistrates to develop a two-step warrant process, whereby a magistrate first issues a warrant authorizing the seizure and then, once there has been an opportunity to more closely assess the reasonableness of searching the seized media, issues a second warrant permitting the search of the seized material. This two-phase system allows for the creation of post-seizure ex ante restrictions that are more likely to create real reductions in privacy cost than merely speculative ones. It is difficult to see what purpose it would serve in an ex post-only regime and so seems to strongly infer that magistrates are authorized to exercise ex ante authority in some cases.

Professor Kerr’s normative criticisms of ex ante restrictions make a persuasive case for at least limiting their use. This Comment shares his concern with the potential for a one-size-fits-all system of ex ante search restrictions (such as the *Comprehensive Drug Testing, Inc.* restrictions) to result in constitutional error. That is why this Comment’s approach ideally places the government in the metaphorical driver’s seat while the magistrate simply serves to let the government know when it has reached the destination. The two-step process implied by Rule 41(e)(2)(B) provides an additional method for reducing constitutional error. Once the computers have been seized, the magistrate is able to make a reasonableness determination with improved information about the amount of information seized and its potential to impose privacy costs. There may even be an opportunity to conduct a full hearing, with briefings from both the government and the suspect regarding the reasonableness of the search. Additionally, once the data has been seized, the magistrate is in a better position to evaluate the effect of government-proposed ex ante restrictions, should they be found to be necessary. The approach advocated in this Comment allows for adaptations that can reduce constitutional error.

---

executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

<sup>226</sup> FED. R. CRIM. P. 41(e)(2)(B).

Similarly, Professor Kerr's concern that permitting ex ante restrictions will retard the development of reasonableness case law in digital search cases is much more applicable to the blanket restrictions imposed by the Ninth Circuit, rather than the approach advocated in this Comment. While it is impossible to know how often magistrates using this Comment's approach would find it necessary to impose ex ante restrictions, it seems unlikely that it will happen in most cases. Magistrates should not entertain ex ante restrictions whenever they feel it would be helpful to do so; they only come into play when the government's requested search would violate the constitution without revision. Furthermore, as Professor Kerr notes in his paper, magistrates can be somewhat cursory in their review of search warrant requests.<sup>227</sup> This would probably result in most digital searches proceeding only with ex post restrictions, with the ex ante restrictions reserved for exceptionally problematic searches, such as the *Comprehensive Drug Testing Inc.* search. Thus, to the extent that ex ante restrictions may limit the ability of appellate courts to develop the law, a majority of digital searches will be likely to be conducted with no ex ante restrictions, providing appellate courts with ample opportunity to develop a case law surrounding the reasonableness of digital searches.

In general, the approach advocated in this Comment seeks to resolve the central problem of digital searches: the creation of circumstances where magistrates must choose between society's need to investigate and deter the growing number of crimes involving computers and the peculiar privacy costs caused by the massive intermingling of data on electronic media. Ex ante restrictions, despite the name, actually serve the purpose of allowing government searches that would not otherwise be permissible to go forward while ensuring that the Fourth Amendment's reasonableness requirements are satisfied. Unlike ex post restrictions, they can be selected based both on their convenience to the investigators and their potential for reductions in privacy cost. They also will tend to provide some guidance to investigators in complex or novel digital investigations, providing a path forward that reduces the risk of an important investigation being sacrificed at the altar of ex post reasonableness case law.

#### E. REASONABLENESS AND PRACTICALITY

The *Comprehensive Drug Testing, Inc.* holding clearly springs from the concern that, by combining plain view with the ostensible need to conduct file-by-file searches, the government has discovered a major

---

<sup>227</sup> See Kerr, *Ex Ante Regulation*, *supra* note 210, at 1283.

loophole to the requirements of the Fourth Amendment.<sup>228</sup> However, it is important not to overestimate the value of this system to the government. Under the plain view doctrine, investigators must have probable cause to believe that an item seized has an “immediately apparent” connection to an illegal act.<sup>229</sup> Traditional examples of items satisfying the requirement include firearms in the homes of known felons, modified rifles, marijuana seeds, and child pornography.<sup>230</sup> In contrast, establishing the requirement for documents seized in plain view can be a very difficult task.<sup>231</sup> Very few computer files are contraband in nature, with child pornography being the primary exception.<sup>232</sup> Similarly, most other files on computers are text-based documents and thus have the same difficulty meeting the requirement as their physical counterparts, namely, the need for further inspection to develop the context for probable cause.<sup>233</sup> For example, an officer searching a computer for evidence of a kidnapping would not find a fraudulent tax return to be immediately apparent.<sup>234</sup> Since the “immediately

---

<sup>228</sup> See *CDT II*, 579 F.3d 989, 999 (9th Cir. 2009) (“The sequence of events supports the suspicion that representations in the warrant about the necessity for broad authority to seize materials were designed to give the government access to the full list of professional baseball players and their confidential drug testing records.”). Judge Kozinski has indicated that his skepticism towards plain view may extend to non-digital contexts as well. See *supra* note 42.

<sup>229</sup> *Arizona v. Hicks*, 480 U.S. 321, 326–27 (1987); *Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971); see also *United States v. Garcia*, 496 F.3d 495, 510 (6th Cir. 2007) (“The immediately apparent requirement is a vital constraint on the plain view exception to the Fourth Amendment warrant requirement.”).

<sup>230</sup> See, e.g., *Washington v. Chrisman*, 455 U.S. 1, 4 (1982) (marijuana seeds); *United States v. Williams*, 592 F.3d 511, 514 (4th Cir. 2010) (machine gun and silencer); *United States v. Lemus*, 582 F.3d 958, 964–65 (9th Cir. 2009) (known felon with firearm); *United States v. Norris*, No. CR 05-2323-TUC-CKJ, 2006 WL 798667, at \*2 (D. Ariz. Mar. 24, 2006) (modified firearm).

<sup>231</sup> See, e.g., *Garcia*, 496 F.3d at 511 (discussing documents requiring “further investigation” and not establishing probable cause of crime upon “immediate sensory perception” not immediately apparent); *United States v. Jimenez*, 205 Fed. Appx. 656, 662 n.2 (10th Cir. 2006) (noting that, “unlike firearms in a felon’s residence, letters do not immediately appear to be evidence of a crime”); *Doane v. United States*, No. 08 Mag. 0017(HBP), 2009 WL 1619642, at \*11 (S.D.N.Y. June 5, 2009); see also *United States v. Hunter*, 13 F. Supp. 2d 574, 586–87 (D. Vt. 1998) (surveying document-based case law predating the probable cause requirement defined in *Hicks*).

<sup>232</sup> See Clancy, *supra* note 125, at 201.

<sup>233</sup> See *Garcia*, 496 F.3d at 511. There are, of course, exceptions to the general rule. See, e.g., *State v. Carroll*, 778 N.W.2d 1 (Wis. 2010) (mobile device seized incident to arrest displays image of owner, a known felon, holding a firearm).

<sup>234</sup> See also Ziff, *supra* note 125, at 869 (positing that investigators undertaking a digital search for child pornography could open a file called “letter-to-grandma.doc” on the grounds that it might contain images of child pornography, but that the investigators could not justify reading any text contained within that document).

apparent” requirement cannot be satisfied retroactively and must be established for every single file seized under plain view, the valid seizure of non-pertinent digital evidence would be rare.<sup>235</sup> Even in *Comprehensive Drug Testing, Inc.*, it is possible that many of the non-BALCO drug records discovered would not meet this test due to legal or legitimate explanations for the test results observed by the officers.<sup>236</sup>

The finite resources of investigators pose an additional limit on digital plain view. As has been noted, pertinent files can easily be disguised and only discovered by a detailed, file-by-file search. However, as memory capacity increases at a rapid pace, such searches become increasingly difficult to perform.<sup>237</sup> File-by-file searches must proceed without regard to file names, formats, or creation dates, since they are premised on the theory that those are unreliable.<sup>238</sup> Indeed, at least one court has concluded that these file-by-file searches cannot open files with names indicative of unrelated crimes, due to the unlikelihood of a criminal disguising a file by giving it an incriminating name.<sup>239</sup> Investigators thus have a strong incentive to avoid conducting file-by-file searches in many instances.

However, each procedure must be transparent for these limitations to be effective. Perjury by officers is a significant threat to Fourth Amendment protections, due to the large number of exceptions to the warrant requirement.<sup>240</sup> Those concerns are heightened in the digital search

---

<sup>235</sup> See *id.* at 867; *United States v. Strand*, 761 F.2d 449 (8th Cir. 1985).

<sup>236</sup> See *CDT I*, 473 F.3d 915, 968 (9th Cir. 2006) (Thomas, J. dissenting) (“It was clear under the testing protocol that positive tests did not necessarily reflect steroid use; the use of nutritional supplements—which is common in professional sports—could also yield a false positive. In addition, there are a whole host of legitimate reasons for individuals to be prescribed steroid products.”).

<sup>237</sup> PETER GRABOWSKY, *ELECTRONIC CRIME* 70 (2d ed. 2007); Ziff, *supra* note 125, at 860–61 (describing a search by the Los Angeles District Attorney’s Office that required 200 terabytes of information to be searched, which is equivalent to a 4,200 mile-high stack of paper). *But see* Kerr, *supra* note 125 at 569–70 (noting that computer searches are somewhat easier to conduct than physical searches of a residence, because they can be done by one person and the search does not have to be done in the field).

<sup>238</sup> See, e.g., *United States v. Gray*, 78 F. Supp. 2d 524, 527 (E.D. Va. 1999) (upholding file-by-file search on grounds that it was conducted systematically, opening files in the order in which they appeared in the directory, regardless of their name); *accord* *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010).

<sup>239</sup> See, e.g., *United States v. Kim*, 677 F. Supp. 2d 930, 950 (S.D. Tex. 2009) (finding that officers conducting a search for documents related to tax fraud lacked probable cause to believe that encrypted files with names suggestive of child pornography might contain information pertinent to their search).

<sup>240</sup> See Stuntz, *supra* note 193, at 938 (“If the law prevents perjury in cases of one type but not of another, a dishonest officer can simply re-describe the case changing his story to take advantage of whatever opportunities the law gives him.”); *see also* Christopher

context, since digital searches are conducted in private settings, where no independent witness can dispute an officer's testimony. Additionally, while a judge may be able to detect inconsistencies in perjured testimony regarding a conventional search, they may have more difficulty doing so in a highly technical context. Therefore, a defendant in a digital search case must be allowed to analyze the search methods used by the government to determine whether the government discovered illicit materials by conducting improper searches—that is, searches that are not conducted in a systematic manner.<sup>241</sup> Technology has made creating these records simple and inexpensive.<sup>242</sup> Recording software can easily and unobtrusively record the process of a hard drive search.<sup>243</sup> Furthermore, the use of bitstream copies allows digital searches to be replicated—a police technician could be asked to state the search procedure that was used to discover a particular piece of evidence and then asked to demonstrate how that evidence was discovered on a copy of the target hard drive.<sup>244</sup> Such a process would give defense counsel many opportunities to detect violations of Fourth Amendment rights and found a suppression motion on it.<sup>245</sup>

Still, even though the potential for widespread abuse of digital plain view is limited by finite resources, it is not a complete solution. Government investigators may hold their resources in reserve, and use them

---

Slobogin, *Testifying: Police Perjury and What to Do About It*, 67 U. COLO. L. REV. 1037 (1996).

<sup>241</sup> For example, abandoning a search for evidence of drug distribution to search for child pornography. *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999).

<sup>242</sup> See, e.g., DemoCreator: Record Everything on Computer Screen and Create Engaged Simulations, WONDERSHARE SOFTWARE, <http://sameshow.com/images/brochure/democreator-brochurex.pdf> (offering retail software for recording computer activity).

<sup>243</sup> *Id.*

<sup>244</sup> Note that this ability to scrutinize the search step-by-step goes a long way towards resolving Judge Kozinski's concerns about abuse of plain view in conventional searches, particularly the ability of officers to lie about how they came to view objects. See *supra* note 41.

<sup>245</sup> However, courts have so far been reluctant to require agents to keep records of search progress and to require those records be provided to defendants. See *United States v. Jack*, No. CR.S-07-0266 FCD, 2009 WL 453051, at \*5 (E.D. Cal. Feb. 23, 2009) (denying a discovery motion for search methodology on grounds that warrant permitted government to open every file on computer); *United States v. Maali*, 346 F. Supp. 2d 1226, 1265 (M.D. Fla. 2004) (finding it unnecessary to maintain record of text searches conducted by agents in face of agent testimony that the searches pertained to the issues raised in the warrant). But see *United States v. Frabizio*, 341 F. Supp. 2d 47, 47 (D. Mass. 2004) (granting motion under FED. R. CRIM. P. 16(a)(1)(E) for discovery of computer search software used by government to scan and detect child pornography on defendant's computer).

to target the unpopular or politically disfavored.<sup>246</sup> The Lerner Formula requirements regarding reasonable searches are therefore indispensable. However, these practical considerations support the proposition that digital data storage and personal computing are not such a radical change from existing criminal procedure doctrine that radically expanded protections are necessary.

## VI. CONCLUSION

The rapid expansion of digital technology and its increasing use does raise serious privacy considerations, including difficult questions concerning government and private data mining,<sup>247</sup> cybervigilantism,<sup>248</sup> searches of digital media incident to arrest,<sup>249</sup> RFID tracking,<sup>250</sup> biometrics,<sup>251</sup> and other technologies.<sup>252</sup> Still, more of our private details

---

<sup>246</sup> See Kerr, *supra* note 125, at 567 (“[T]he ability to engage in pretextual searches may permit the police to target unpopular or politically powerless persons or groups for heightened scrutiny . . . . This discriminatory and inefficient practice was just the kind of misuse of government power the Fourth Amendment was created to stop.”). Arguably, the federal investigation into Allegheny County Coroner Cyril Wecht represents an example of this kind of abuse. See *United States v. Wecht*, 619 F. Supp. 2d 213, 248 (W.D. Pa. 2009) (finding warrant permitting seizure of laptop and all data stored within laptop overbroad in a political corruption case); *Allegations of Selective Prosecution: The Erosion of Public Confidence in Our Federal Justice System: Hearing Before the H. Comm. On the Judiciary*, 101st Cong. (2007) (Testimony of Fmr. Att’y Gen. Dick Thornburgh) (suggesting that the prosecution of County Coroner Wecht, a Democrat, by a Republican U.S. Attorney was politically motivated); Jason Cato, *Prosecution’s Conduct in Wecht Case Labeled “Troubling,”* PITTSBURGH TRIBUNE-REV. (Apr. 12, 2008), [http://www.pittsburghlive.com/x/pittsburghtrib/news/s\\_562027.html](http://www.pittsburghlive.com/x/pittsburghtrib/news/s_562027.html).

<sup>247</sup> See SOLOVE, *supra* note 142; Christopher W. Clifton, et al., *Data Mining and Privacy: An Overview*, in *PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION* 191 (Katherine Strandburg & Daniela Stan Raicu eds. 2006).

<sup>248</sup> See *United States v. Jarrett*, 338 F.3d 339 (4th Cir. 2003); *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003); PETER GRABOSKY, *ELECTRONIC CRIME* 98–102 (2006).

<sup>249</sup> See Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 *UCLA L. REV.* 27 (2008); see, e.g., *United States v. Reynolds*, No. 3:08-CR-143, 2009 U.S. Dist. LEXIS 71057 (E.D. Tenn. June 4, 2009).

<sup>250</sup> See Ari Juels, *RFID Privacy: A Technical Primer for the Non-Technical Reader*, in *PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION* 57–73 (Katherine Strandburg & Daniela Stan Raicu eds. 2006). RFID is an acronym for “Radio-Frequency Identification.” An “RFID tag” is a tiny, inexpensive chip that transmits a uniquely identifying number over short distances. *Id.* at 57. Their increasing ubiquity is raising privacy concerns in several areas. See, e.g., M.L. Wald, *New High-Tech Passports Raise Concerns of Snooping*, *N.Y. TIMES*, Nov. 26, 2004, at 28.

<sup>251</sup> See Lisa S. Nelson, *Constructing Policy: The Unsettled Question of Biometric Technology and Privacy*, in *PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION* 152–72 (Katherine Strandburg & Daniela Stan Raicu eds.,

are becoming digitized. Technology will continue to develop new ways that that information can be stored, distributed, seized and stolen. Therefore, it is important that the courts adopt a flexible approach, similar to the flexible approach used in many conventional searches. By working to balance public interests with privacy interests on a case-by-case basis, magistrates can encourage the efficient administration of justice and constitutional protections. While *Comprehensive Drug Testing, Inc.* proposes a solution that may work in extreme cases, it is not appropriate in all cases. Its impracticality risks ceding the argument to the more conventional approaches of the Fourth and Seventh Circuits, which themselves may be inadequate to protect Fourth Amendment rights in all cases. A flexible approach based on balancing of interests presents the most sustainable option for courts seeking to address the Fourth Amendment concerns raised by digital searches.

---

2006). Popular culture has begun to reflect concerns regarding biometric privacy. *See, e.g.*, MINORITY REPORT (Amblin Entertainment 2002).

<sup>252</sup> *See* U.S. v. Riley, 906 F.2d 841, 853–55 (2d Cir. 1990) (Weinstein, J. dissenting) (listing technological improvements in forensic science and expressing concern about the Fourth Amendment implications of their aggregated use).