Harvard Journal of Law & Technology
Volume 23, Number 2 Spring 2010

SEPARATING HARD FACT FROM HARD DRIVE: A SOLUTION FOR PLAIN VIEW DOCTRINE IN THE DIGITAL DOMAIN

*Andrew Vahid Moshirnia**

TABLE OF CONTENTS

I. INTRODUCTION 610

II. THE PLAIN VIEW DOCTRINE AND DIGITAL SEARCHES 611
A. Facts of Comprehensive Drug Testing 613
B. Facts Relating to Federal Rule of Criminal Procedure Rule 41 616

II. THE CONFLICT BETWEEN RULE 41 AND *CDT II* 617
A. Direct Conflict Between Rule 41 and CDT II 618
B. Courts Are Likely To Apply Rule 41, in Conflict with CDT II 619
C. Practical Necessity as Motivation for Avoiding CDT II 620
D. Courts Are Unlikely To Adopt CDT II Outside the Medical Context 621

III. FLAWED ALTERNATIVES: OTHER SUGGESTIONS FOR RESOLVING THE ELECTRONIC PLAIN VIEW PROBLEM 622
A. The Permissive Container Approach 622
B. Intent-Based Approach of Carey 623
C. Technological Solutions 624

IV. A BETTER APPROACH: BALANCING SOCIETY'S INTEREST IN PREVENTING UNDERLYING CRIME AGAINST THE DEFENDANT'S INTEREST IN SEARCHED MATERIAL 626
A. Balancing Test Best Serves Purposes of Plain View Doctrine 626
B. Applying the Balancing Test 627
1. Society's Interest in Preventing the Underlying Crime 628
2. Individual Privacy Interest in Searched Material 628
3. Case Studies 630

* Harvard Law School, Candidate for J.D., 2011, University of Kansas, Ph.D., 2008. I would like to thank Professors Brian Sheppard, Phil Malone, and Alex Whiting for their invaluable assistance.

C. Comporting with Rule 41 and Horton.....631
D. Preserving Case Outcomes While Formulating a Coherent Standard.....632
E. Avoiding a Statutory Definition.....632

V. CONCLUSION.....633

I. INTRODUCTION

In a two-day span, two different circuit splits developed over the issue of how to interpret the plain view doctrine for digital searches.[1] The judiciary has struggled for more than a decade with the application of the plain view doctrine in an electronic world.[2] However, the courts' attempts to adopt a constitutionally robust or logically coherent approach to computer searches within the doctrine's framework have met with failure.

A recent decision by the Ninth Circuit highlights this discord. In *United States v. Comprehensive Drug Testing*,[3] or "*CDT II*," the court, sitting en banc, set forth heightened procedural and particularity requirements for the search and seizure of digital evidence.[4] In so doing, the Ninth Circuit ignored the practical necessities of law enforcement as well as the preferences of the Supreme Court and instead adopted a sweeping ban that forbids the search of any file not specifically mentioned in a warrant.[5] The Ninth Circuit rule effectively rejects the plain view doctrine for electronic searches. The vitality of this decision both within and outside of the Ninth Circuit is unclear in light of recent judicial rulemaking. Specifically, the requirements announced in *CDT II* conflict with the latest revision of Rule 41 of the Federal Rules of Criminal Procedure ("FRCrP") that became effective December 1, 2009. This creates the potential problematic situation of a court ignoring — and implicitly questioning the constitutionality of — an approved but not yet enacted Federal Rule.

---

1. United States v. Williams, 592 F.3d 511, 514 (4th Cir. 2010) (holding, in the alternative, that plain-view exception applies to digital searches); United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010) (upholding a digital search as being within the scope of the issued warrant, but warning investigators that certain exceptions to the warrant requirement were not applicable under the circumstances); *see also* Posting of Orin Kerr to The Volokh Conspiracy, Plain View for Computer Searches Generates Two Circuit Splits in Two Days: *United States v. Williams* and *United States v. Mann*, http://volokh.com/2010/01/21/plain-view-for-computer-searches-generates-two-circuit-splits-in-two-days-united-states-v-williams-and-united-states-v-mann/ (Jan. 21, 2010, 23:41 EST).

2. *See infra* Part II.

3. 579 F.3d 989 (9th Cir. 2009) (en banc). For ease of reference, this Note will refer to the earlier panel decision in the case, 513 F.3d 1085 (9th Cir. 2008), as "*CDT I*," and the later en banc decision as "*CDT II*."

4. *CDT II*, 579 F.2d at 989–98, 1000.

5. *Id.* at 1000.

This Note argues that the *CDT II* factors are doomed to fail. First, courts are unlikely to disregard the Federal Rules of Criminal Procedure in applying these factors. Second, the *CDT II* factors are unworkable outside of the medical context. Nor does Rule 41 provide a workable approach to digital search and seizure. Rather, Rule 41 creates a void in Ninth Circuit precedent that the *CDT II* rule fails to fill. Rule 41 does not provide a well-reasoned search approach but merely codifies the ambiguous status quo in allowing expansive and rudderless electronic searches. Just as *CDT II*'s approach is too strict, Rule 41's approach is too lax. Both of these flaws evince the incompatibility of the physical doctrine with the electronic world.

This Note presents a much-needed new approach. There are already a handful of alternatives to the electronic plain view doctrine — such as intent-based and technology-based approaches — but their costs outweigh their benefits. The best framework is a balancing test that weighs the seriousness of the crime alleged against the importance of the privacy interests threatened by the search. It achieves the underlying goals of the plain view doctrine without resorting to a cumbersome conflation of the physical and the electronic.

Part II of this Note discusses the difficulty of applying the plain view doctrine to digital searches and explores *CDT II* and Rule 41 as proposed solutions to that problem. Part III discusses the conflict between *CDT II* and Rule 41 and concludes that *CDT II* cannot survive the adoption of Rule 41. Part IV examines three attractive, but ultimately flawed, approaches to the electronic plain view doctrine. Part V proposes a new balancing test to solve the electronic plain view problem.

II. THE PLAIN VIEW DOCTRINE AND DIGITAL SEARCHES

The Fourth Amendment prohibits unreasonable search and seizure.[6] Accordingly, officers must show probable cause to obtain a warrant, which must be narrowly tailored.[7] Warrants not only limit the kinds of evidence that officers may seize, but also restrict the areas officers may search.[8] However, officers may also seize evidence that is in plain view during their searches, provided that officers encounter this evidence during their authorized search and that the incriminating nature of the evidence is "immediately apparent."[9]

---

6. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

7. Groh v. Ramirez, 540 U.S. 551, 556–57, 561–63 (2004).

8. *See id.*

9. Horton v. California, 496 U.S. 128, 135–36 (1990) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971)).

Though the plain view doctrine increases the amount of evidence an officer can possibly seize, it also limits the manner in which the police conduct searches. If an officer conducts an unreasonable search, such as looking for a large gun in a very small bag, any evidence seized from that unwarranted search may be suppressed.[10] The doctrine is only satisfied when the officer conducts a narrowly tailored search reasonably related to the discovery of target evidence. For example, if a police officer encounters pornographic pictures of minors while searching for illegal narcotics in a suspect's dresser, the officer could seize the pictures so long as she could justify the search of the dresser.

The requirements of the plain view doctrine — that an incriminating item be housed in an area specified in a delimited warrant and that it be in the plain view of investigating officers — simply do not translate to a digital environment. Officers neither stand within the confines of the computer nor rely on their ambient vision to immediately identify elements of the digital landscape. Instead, officers interact with the contents of a computer in a very abstract and mediated way. A user must execute a file to reveal its hidden contents. Accordingly, a directory is not obviously incriminating until it is investigated.

The fragmented and decompartmentalized nature of computer data further complicates electronic plain view. The rooms of a home or building typically serve as the units of area for a search warrant.[11] However, there is no analogous structure in a hard drive. Courts still struggle to define the unit of approach in digital searches. Some courts use a physical container approach and analogize whole hard drives to containers or cabinets — once a drive is accessed, officers may inspect all files therein.[12] Other courts use a file approach and analogize individual files to containers — officers must follow a defined search protocol designed to uncover incriminating files.[13] But any analogy to the physical world is difficult to draw because conventional measures such as size or appearance do not ultimately constrain the placement of data.[14]

The plain view doctrine in electronic searches presents a particularly difficult problem because narrowly tailored examinations of computers are impractical. Though a warrant may describe a certain

10. *See, e.g.*, Arizona v. Hicks, 480 U.S. 321, 324–25 (1987) (moving shooting suspect's stereo in order to record serial numbers without probable cause forced suppression of evidence). This exclusionary rule is subject to the "inevitable discovery exception," which allows evidence that would have been uncovered eventually to be admitted regardless of whether its discovery was in good faith. Nix v. Williams, 467 U.S. 431, 444 (1984).

11. *See* Orin S. Kerr, Essay, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 290–92 (2005).

12. *See, e.g.*, United States v. Runyan, 275 F.3d 449, 462 (5th Cir. 2001). *See generally* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

13. *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1273–75 (10th Cir. 1999).

14. For example, users may employ compression to adjust a file's size.

type of file, for example a text file, it is difficult to conduct a search only of text files.[15] Users may easily hide files by misnaming or removing extensions.[16] Furthermore, an officer may have to use other files in order to decrypt or decompress the target file.[17] Therefore, a search for a single digital file may necessitate the search and seizure of all files in a computer.[18]

But due to the plain view doctrine, police may seize and act upon any of these examined files. In short, a narrowly tailored warrant authorizing the seizure of a single file from a single hard drive nevertheless may enable officers to seize all files and, by extension, all of a defendant's hard drives. This practice is especially worrisome when a single drive commingles the information of many different individuals, as is the case in many medical or corporate databases.[19]

Because the plain view doctrine is discordant with the digital domain, courts have struggled to apply their prior physical jurisprudence to new technologies. While some courts have become so frustrated that they have effectively abandoned plain view in the electronic context, other courts have adopted tortured and ultimately unsatisfactory frameworks for digital searches. In the following Subpart, this Note discusses an important recent example of the former.

A. Facts of Comprehensive Drug Testing

The *CDT* cases grew out of an investigation into Major League Baseball's ("MLB") steroid problem. The federal government has repeatedly expressed concern over the use of illegal performance enhancing drugs in professional sports.[20] In 2002, the government began investigating the Bay Area Lab Cooperative's ("Balco") connection with the distribution of steroids to professional athletes.[21] In that same year, MLB and the Major League Baseball Players Association ("Players Association") agreed to an anonymous and confidential drug testing regime of all players.[22] The players were promised that the results of these drug tests would remain confidential.[23] MLB contracted with Comprehensive Drug Testing, Inc. ("CDTI") to oversee

15. *CDT II*, 579 F.3d 989, 995 (9th Cir. 2009) (en banc).
16. *Id.*
17. *Id.*
18. *See id.*
19. The Ninth Circuit addressed the problem of commingling in *United States v. Tamura*, 694 F.2d 591, 595–96 (9th Cir. 1982), but that case preceded the widespread use of computers and instead focused on the seizure of paper documents.
20. *See, e.g.*, Anabolic Steroids Control Act of 2004, Pub. L. No. 108-358, 118 Stat. 1661; Anabolic Steroids Control Act of 1990, H.R. 4658, 101st Cong. (1990); *see also* Rick Collins, *Changing the Game: The Congressional Response to Sports Doping via the Anabolic Steroid Control Act*, 40 NEW ENG. L. REV. 753, 754–58 (2005).
21. *CDT I*, 513 F.3d 1085, 1089 (9th Cir. 2008).
22. *CDT II*, 579 F.3d 989, at 993.
23. *Id.*

the program and with Quest Diagnostics ("Quest") to analyze players' urine samples.[24]

The government's investigation of Balco continued for several years; in 2004, the government subpoenaed CDTI and Quest for the test results of eleven MLB players.[25] The Players Association and Quest moved to quash these subpoenas.[26] Before their motions were granted, the government obtained warrants pertaining to CDTI's office in Long Beach, California and Quest's lab in Las Vegas, Nevada.[27] The warrants approved the "seizure of drug testing records and specimens for ten named Balco-connected players."[28] Because these records were likely to be stored on computers, the warrants authorized the search of computer equipment. The warrant provided that: (1) "computer personnel" would determine the most prudent way to gather the desired information, including onsite data copying and equipment seizure; and (2) these personnel would be authorized to search the entirety of the data "authorized by the warrant," including data that had been copied onsite. [29]

The government executed a search on CDTI's office and discovered "a computer directory containing all of the computer files for [CDTI]'s drug testing programs."[30] Though the government's warrant mentioned only ten players, the government used information from this directory to apply for new warrants to seize records for all other players who had returned positive results.[31] These warrants were granted and executed.[32] Subsequently, the government issued grand jury subpoenas to gather similar information.[33]

In response, the Players Association and CDTI moved for the return of seized data and equipment under FRCrP 41(g) in both California and Nevada.[34] In California, these parties also moved under FRCrP 17(c) to quash the subpoenas resulting from the search.[35] All of these motions were granted on the basis that the searches were improper. Judge Cooper in California found that the government's actions failed to follow precedent;[36] Judge Mahan in Nevada found that they "callously disregarded . . . constitutional rights";[37] and Judge

24. *Id.*
25. *CDT I*, 513 F.3d at 1090.
26. *Id.* at 1091.
27. *Id.*
28. *Id.*
29. *Id.* at 1092–93.
30. *Id.* at 1092.
31. *Id.* at 1094.
32. *Id.*
33. *Id.* at 1095.
34. *CDT II*, 579 F.3d 989, 993–94 (9th Cir. 2009) (en banc).
35. *Id.* at 994.
36. *CDT I*, 513 F.3d at 1095.
37. *Id.* at 1094.

Illston in California found the government's actions to be "harassment."[38] Further, Judge Illston noted that the subpoenas were redundant and were likely intended to grant an aura of legality to information obtained illegally.[39] The Government appealed all three decisions to the Ninth Circuit, which upheld Judge Cooper's order.[40] However, the court reversed Judge Mahan's order and Judge Illston's order to quash.[41]

In August 2009, the Ninth Circuit, sitting en banc, reversed the portion of the panel's decision concerning Judge Mahan's and Judge Illston's orders.[42] Chief Judge Kozinski, writing for the majority, focused on the risks of bootstrapping and overreaching in cases involving digital evidence and laid out five factors for future cases:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction must be either 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.
>
> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.[43]

To date, no published case has applied these factors.

---

38. *Id.* at 1095.
39. *Id.* at 1127.
40. *Id.* at 1116.
41. *Id.*
42. *CDT II*, 579 F.3d 989, 1007 (9th Cir. 2009) (en banc).
43. *Id.* at 1006 (citations omitted).

B. Facts Relating to Federal Rule of Criminal Procedure Rule 41

The Ninth Circuit is not the only judicial body to address the growing question of electronic searches. In March 2009, the Supreme Court adopted several new amendments to the FRCrP pursuant to 28 U.S.C. § 2072.[44] These amendments took effect on December 1, 2009.[45] This slate of changes included a significant revision of Rule 41, putting forth several new guidelines for searches involving digital evidence:

> [41(e)](2) Contents of the Warrant.
>
> (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. . . .
>
> . . . .
>
> (B) Warrant Seeking Electronically Stored Information. 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 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.
>
> . . . .
>
> [41](f) Executing and Returning the Warrant.
>
> (1) Warrant to Search for and Seize a Person or Property.
>
> . . . .

44. FED. R. CRIM. P. historical note at XIII.
45. *Id.*

> (B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.[46]

Scholars have yet to fully address the impact of the enactment of Rule 41 on the *CDT II* factors.[47]

II. THE CONFLICT BETWEEN RULE 41 AND *CDT II*

CDT II is binding within the Ninth Circuit, as are the Federal Rules with respect to criminal proceedings.[48] While some portions of the new Rule 41 and *CDT II* can be read to complement one another, other parts are in direct conflict. In resolving the conflict, courts will look to whether the Ninth Circuit based its decision in *CDT II* on supervisory powers, in which case Rule 41 trumps, or on constitutional powers, in which case *CDT II* trumps.[49] While it is not entirely clear how these issues will be resolved, it seems likely that courts within the Ninth Circuit will determine *CDT II* to be supervisory, and will follow Rule 41, at least where the sets of rules conflict.

---

46. FED. R. CRIM. P. 41(e)(2)–(f)(1)(B).

47. Analysis of the 2009 amendments to Rule 41 has focused on the issue of whether a government's creation of a perfect copy of user data rises to the level of seizure. Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010); Mark Taticchi, Note, *Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 GEO. WASH. LAW REV. 476 (2010). Case comments on *CDT II* have largely ignored the possible impact of the 2009 FRCrP amendments. *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) [hereinafter "Recent Case: CDT II"].

48. *See* FED. R. CRIM. P. 1(a)(1) ("These rules govern the procedure in all criminal proceedings in the United States district courts, the United States courts of appeals, and the Supreme Court of the United States.").

49. *See infra* note 58 and Part II.B.

A. Direct Conflict Between Rule 41 and CDT II

Rule 41 and *CDT II* have irreconcilable approaches to the storage of data by law enforcement officials and the scope of electronic searches. *CDT II* Factor 5 states that "[t]he government must destroy or, if the recipient may lawfully possess it, return non-responsive data."[50] This directly conflicts with Rule 41(f)(1)(B), which states that "[t]he officer may retain a copy of the electronically stored information that was seized or copied."[51]

Further, *CDT II* Factor 4 provides: "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."[52] This implies that the unit of approach is the file rather than the physical container. The file approach is designed to limit the scope of the search to certain files, whereas the physical approach allows for the search of all files in a single storage medium.[53] While Rule 41 is largely silent on the plain view doctrine, several considerations suggest that Rule 41 supports the continued use of the plain view doctrine and the physical container approach. First, the Rule specifically states that any inventory of seized items need not include the names of actual files; rather "the inventory may be limited to describing the physical storage media that were seized or copied."[54] This implies that an officer is expected to seize data containers and search their entire contents. Furthermore, the Rule allows officers to "retain a copy of the electronically stored information that was seized or copied";[55] this fact hints that the container is the appropriate unit of approach because the method of data copying involves taking an entire disk image.[56] Finally, the Rule's silence on the plain view doctrine implies that the practice may continue.[57]

---

50. *CDT II*, 579 F.3d 989, 1006 (9th Cir. 2009) (en banc).

51. FED. R. CRIM. P. 41(f)(1)(B).

52. *CDT II*, 579 F.3d at 1006.

53. *Compare* United States v. Carey, 172 F.3d 1268, 1272–76 (10th Cir. 1999) (applying the file approach), *with* United States v. Runyan, 275 F.3d 449, 463–66 (5th Cir. 2001) (applying the physical approach). *See generally* discussion *infra* Part III.B.

54. FED. R. CRIM. P. 41(f)(1)(B).

55. *Id.*

56. Of course the dominant method of data copying could change. For example, officers could request specific files from Internet Service Providers. However, bitstream copying of a suspect's hard drive was the common method of data seizure at the time of the drafting of the Rule, so this section of the Rule likely endorses a container approach. *See* United States v. Mann, 592 F.3d 779 (7th Cir. 2010) (allowing evidence of child pornography found by coping defendant's computer hard drives and searching for voyeuristic images).

57. *CDT II* and the new Rule 41 do not conflict in all respects. Thus, courts within the Ninth Circuit might initially seek to satisfy both standards, by adhering to the *CDT II* restrictions that do not expressly conflict with Rule 41. For example, courts could keep in use the heightened protections found in *CDT II* Factors 1–3 (relinquishing plain view; the use of third parties for redaction or segregation; risk of data destruction and previous attempts to obtain data) but discard the other factors and instead employ the more lenient retention

To resolve these conflicts between *CDT II* and Rule 41, the key question courts must address is whether *CDT II* was based on supervisory powers or on constitutional analysis. If the ruling was based on the court's supervisory powers, then the Federal Rule trumps the decision.[58] If the ruling was based on an analysis of the Fourth Amendment, then the ruling (as a correction of a constitutional infirmity) trumps the Federal Rule, at least within the Ninth Circuit.

B. Courts Are Likely To Apply Rule 41, in Conflict with CDT II

In determining whether *CDT II* was based on supervisory powers or constitutional analysis, courts will look both to the opinion itself and to pragmatic considerations. While the opinion itself is not entirely clear, it seems likely that courts will determine the decision to be based on supervisory powers and therefore will follow Rule 41 where it conflicts with *CDT II*.

In *CDT II*, Judge Kozinski hinted at constitutional analysis by stating that only clear rules can safeguard the privacy rights enshrined in the Fourth Amendment: "Everyone's interests are best served if there are clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment."[59]

However, Judge Kozinski never engaged the Constitution directly. He did not conduct a robust proportional analysis to determine what level of privacy protection was required, nor did he explain search practices in terms of constitutional infirmity. Instead, he framed the new restrictions as an update of *United States v. Tamura*,[60] which laid out guidelines for the rapid segregation and return of seized, intermingled documents.[61] Because *Tamura* is a supervisory guidepost offering a "solution to the problem of necessary overseizing of evidence,"[62] it is likely that courts will view *CDT II* as an extension of *Tamura* built on supervisory powers. In addition, he sug-

---

standards in Rule 41 (data allowed to be copied and retained). Eventually, however, it is likely that courts will move away from *CDT II* in favor of Rule 41 due to practical concerns.

58. *See* United States v. Payner, 447 U.S. 727, 735 n.8 (1980) ("We . . . reject [supervisory powers'] use as a substitute for established Fourth Amendment doctrine.").

59. *CDT II*, 579 F.3d 989, 1006 (9th Cir. 2009) (en banc).

60. 694 F.2d 591 (9th Cir. 1982).

61. *See id.* at 595–97 (stating that authorities should avoid seizing intermingled documents and in the event of over-seizure should quickly segregate and return documents not mentioned in the warrant).

62. *CDT II*, 579 F.3d at 1006. Because the over-seizure portion of *Tamura* is based on the American Law Institute's Model Code of Pre-Arraignment Procedure, *see Tamura*, 694 F.2d at 596 & n.3, rather than explicit constitutional analysis, that part of the opinion should be interpreted as flowing from the court's supervisory powers. However, *Tamura* does contain some elements of constitutional analysis, *see id.* at 595, so it is possible that courts could disagree as to the basis of *Tamura*.

gested that the restrictions in *CDT II* are prospective by noting that "the procedures . . . outlined above will prove a useful tool *for the future*."[63] Prospective opinions are almost always supervisory, in contrast to constitutional opinions that seek to correct a *current* constitutional infirmity.[64]

C. Practical Necessity as Motivation for Avoiding CDT II

Pragmatic considerations will also motivate courts in the Ninth Circuit to find that *CDT II*'s factors are supervisory dicta, clarified or overruled by the Federal Rules.[65] If the factors set out in *CDT II* are designed to correct deficiencies in electronic searches and to prevent Fourth Amendment infirmities, then it follows that these requirements are retroactive and that previous searches[66] (or at least previous searches in cases that have not yet been adjudicated) were constitutionally deficient.[67] Courts will want to avoid this result in order to prevent a flurry of related litigation.[68] It also is unclear if law enforcement officials will be able to comply with the *CDT II* requirements due to manpower and expertise shortages.[69]

---

63. *CDT II*, 579 F.3d at 1006–07 (emphasis added).

64. *See* Griffith v. Kentucky, 479 U.S. 314, 328 (1987).

65. An alternative would be to ignore *CDT II* entirely. This may be that the approach that the courts are already taking. For example, in *United States v. Roller*, No. CR-08-00361-RMW, 2009 WL 3762417 (N.D. Cal. Nov. 9, 2009), a district court ruled that a warrant authorizing a search of the defendant's computer for child pornography was not defective even though the warrant failed to adequately particularize the items to be seized. "[S]ince the scope of what was the subject of the search was limited to materials constituting evidence of offenses related to child pornography, the warrant was not overbroad." *Id.* at *5. The court did not cite *CDT II* but instead based the ruling on *United States v. Hay*, 231 F.3d 630 (9th Cir. 2000). *Id.*

66. It seems that *CDT II* would not qualify as a watershed rule, and thus would not apply retroactively to adjudicated cases, under the two part test set out in *Teague v. Lane*, 489 U.S. 288, 311 (1989). Though the *CDT II* factors may be considered essential to "fundamental fairness" in the justice system, they do not appear to prevent "an impermissibly large risk that the innocent will be convicted." *Teague*, 489 U.S. at 312 (quoting Desist v. United States, 394 U.S. 244, 262 (1969)).

67. *Griffith*, 479 U.S. at 322 ("[F]ailure to apply a newly declared constitutional rule to criminal cases pending on direct review violates basic norms of constitutional adjudication.").

68. Courts have generally avoided manner-specific warrants, thereby "le[aving] to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant." Dalia v. United States, 441 U.S. 238, 257 (1979); *see also* United States v. Graziano, 558 F. Supp. 2d 304, 315–16 (E.D.N.Y. 2008) (refusing to adopt a rule invalidating a search warrant simply because it does not indicate the search procedure for a target computer); United States v. Hill, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004) (Kozinski, J., by designation) (declining to find a warrant overbroad because it did not include a search methodology).

69. *See* Brief for the United States in Support of Rehearing En Banc by the Full Court at 15–18, *CDT II*, 579 F.3d 989 (9th Cir. 2009) (No. 05-55354). *See generally* Derek Regensburger, *Bytes, BALCO, and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in* United States v. Comprehensive Drug Testing, Inc., 97 J. CRIM. L. & CRIMINOLOGY 1151 (2007).

D. Courts Are Unlikely To Adopt CDT II *Outside the Medical Context*

Though the Ninth Circuit expressly stated that the *CDT II* factors were to apply to all digital searches, it is far more likely that courts will attempt to limit the application of *CDT II* to its facts — commingled medical files. The medical context of *CDT II* highlights the disconnect between the goal of the *CDT II* restrictions — protecting the justified privacy of third parties — with the goals of digital cases that involve the privacy concerns of only one user. For example, digital searches for drug crimes often uncover evidence of child exploitation; here, society's interest in protecting the well-being of children and detecting the criminal activity of third parties takes precedence over the privacy of the suspect. Though there are many other sources for possible digital seizure regimes, circuits might look to *CDT II* for guidance in cases involving medical privacy.[70] However, courts both inside and outside of the Ninth Circuit will likely recognize the restrictions' poor fit for child exploitation cases[71] and limit *CDT II*'s application to medical searches only.

For all of these reasons, courts within the Ninth Circuit are likely to apply Rule 41 rather than *CDT II*, at least where the two approaches directly conflict. Where there is no direct conflict, courts within the Ninth Circuit may at least initially try to apply both. However, due to the unique factual situation at issue in *CDT II*, the *CDT II* factors may have greater impact in medical cases than in other contexts.[72] Furthermore, courts outside of the Ninth Circuit are unlikely to adopt the *CDT II* factors. As in the Ninth Circuit, other courts are likely to interpret the *CDT II* factors as flowing from supervisory powers, rather than from constitutional analysis.[73] Moreover, there are

---

70. Numerous commentators have highlighted the need for specialized rules in digital evidence cases, especially in the medical context. *See, e.g.*, RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31 (2007); Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 102 (2005). These commentators posit that there is a direct conflict between the goals of plain view doctrine and the promise of digital privacy. The Ninth Circuit focused on this tension and drafted the *CDT II* restrictions accordingly. *See CDT II*, 579 F.3d 989, 998 (9th Cir. 2009) (en banc).

71. This Note only briefly considers the specific practical concerns that would result from widespread adoption of *CDT II* in other contexts. It is likely that labs, already short of examiners, would simply be unable to comply with *CDT II*. *See, e.g.*, Posting of Joel Rubin to L.A. Now, LAPD's Crime Lab Hampered By DNA Backlog, Money Woes, http://latimesblogs.latimes.com/lanow/2010/01/lapd-crime-lab-hampered-by-backlog-money-woes.html (Jan. 15, 2010, 11:05 PST). In cases where a cipher or code is used in a communication, an examiner may require an officer's expertise. Further, a regime that mandates the deletion of seized files can be attacked on the grounds that it will destroy both exculpatory and inculpatory evidence.

72. *See supra* Part II.D.

73. *See supra* note 58 and Part II.B .

several alternate sources for digital evidence rules, including the Federal Rules and precedent from other circuits.[74]

III. FLAWED ALTERNATIVES: OTHER SUGGESTIONS FOR RESOLVING THE ELECTRONIC PLAIN VIEW PROBLEM

The Ninth Circuit's new regime governing the search and seizure plain view digital evidence likely will not endure. This uncertainty in the future of the law necessitates consideration of other solutions to the electronic plain view problem. Some courts have simply ignored the issue by treating computers as rooms or containers and imposing no restrictions on electronic plain view.[75] Others have attempted to address the problem of applying a physical doctrine to a digital setting by focusing on the intent of investigators.[76] Scholars have also offered fixes, seeing promise in technological filters of data.[77] Though initially these approaches seem appealing, none provide a satisfactory solution. This Part discusses these three approaches and critiques their flaws.

A. The Permissive Container Approach

Several circuits have already articulated a specialized regime for the search and seizure of digital evidence.[78] The Fifth Circuit adopted the physical container approach in *United States v. Runyan*.[79] There, the court held that, where the defendant's estranged wife had already accessed a limited number of files on the defendant's computer disks, a police search of different files on those disks did not constitute a new search but merely expanded the prior search.[80] Under this scheme, data storage devices are treated as containers; once a single file on that container is accessed, the entire device is open to search and seizure.

While this approach provides a bright line rule — a warrant for one file is a warrant for all files on a device — the legal fiction of treating computers like cans does little to address a suspect's privacy concerns or the concerns of other individuals with commingled data. As a result, this approach could prove disastrous in the medical or corporate contexts because it is likely allow searches of individuals'

74. *See, e.g.*, United States v. Mann, 592 F.3d 779, 784 (7th Cir. 2010) (applying the inadvertence standard of *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), while expressly disagreeing with the pre-approval requirements suggested in *CDT II*).

75. *See infra* Part III.A.

76. *See infra* Part III.B.

77. *See infra* Part III.C.

78. *See generally* Kerr, *supra* note 11.

79. 275 F.3d 449, 463–64 (5th Cir. 2001).

80. *Id.* at 452–53, 464–65.

private information that is only tenuously related to the criminal investigation. In addition, new forms of data storage will make this approach more difficult to execute. Server side hosting of data means that information may be in multiple locations. In short, it will become difficult to identify the container to search.

B. Intent-Based Approach of Carey

In contrast to the permissive container approach, the Tenth Circuit adopted the individual file approach in *United States v. Carey*.[81] There, the government searched the defendant's computer for evidence of drug dealing.[82] In the course of the search, an officer discovered 244 images of child pornography.[83] The Tenth Circuit held that the first image of pornography that the officer discovered could be seized under the plain view doctrine.[84] However, the remaining 243 images could not be seized because the officer altered his search and expected to find child pornography.[85] Accordingly, the Tenth Circuit adopted a digital search regime that would exclude digital evidence that was discovered by an officer intending to uncover incriminating evidence outside of the scope of the warrant. In effect, the digital discovery must be inadvertent to be admissible. Though this technique could deter some pretextual searches,[86] it is neither practical nor consistent with the greater body of Fourth Amendment jurisprudence.[87]

The difficulty of determining an officer's subjective intent partially motivated the Supreme Court's emphatic rejection of an intent-based rule for plain view evidence. This view was clearly stated in *Whren v. United States*: "Not only have we never held . . . that an officer's motive invalidates objectively justifiable behavior under the Fourth Amendment[] . . . we have repeatedly held and asserted the contrary."[88] The Court also explicitly rejected any intent or inadvertence test for plain view evidence in *Horton v. California*,[89] though

81. 172 F.3d 1268 (10th Cir. 1999).
82. *Id.* at 1270–71.
83. *Id.* at 1271.
84. *Id.* at 1273 & n.4.
85. *Id.*
86. *See* Horton v. California, 496 U.S. 128, 140–41 (1990) (discussing the partial but ultimately inadequate protection afforded by the inadvertence requirement).
87. *See* United States v. Williams, 92 F.3d 511, 522–23 (4th Cir. 2010) (expressly disagreeing with the subjective intent test of *Carey* in light of the Supreme Court's holding in *Horton*). *But see* United States v. Mann, 592 F.3d 779, 784–85 (7th Cir. 2010) (adopting an inadvertence standard while expressly disagreeing with pre-approval requirements suggested in *CDT II*).
88. 517 U.S. 806, 812 (1996).
89. *Horton*, 496 U.S. at 140 ("[N]o additional Fourth Amendment interest is furthered by requiring that the discovery of [plain view] evidence be inadvertent.").

Justice Brennan noted that pretextual searches could pose a threat to suspects' Fourth Amendment rights.[90]

The subjective intent of an officer can be incredibly difficult to discern.[91] For example, files may bear misleading names or file extensions. Therefore, a search through a certain type of file is not dispositive of an officer's intent. The only reliable evidence of subjective intent is an admission from the investigating officer — a rare event indeed. Of course, in *Carey*, the officer admitted that he deviated from his search and began looking at the defendant's photos in order to discover illicit pornographic images.[92] Absent this admission, it seems likely that the court would not have suppressed the evidence.[93] Surely, we can expect that it would be unusual for this kind of admission to recur.

C. Technological Solutions

The solution to this problem may not come from previous court opinions. Commentators have remarked that more powerful search or filter software could solve the problem of the plain view doctrine in the digital context.[94] In this scenario, a tool could immediately discern the true type of each file and thus remove the necessity of the officer's examining each file.[95] A shortcut to this result is not to develop an all-powerful search tool but rather to confine searches to "responsive files," or files that can be opened using specific programs contained on the suspect's computer.[96]

These technological approaches are inherently flawed. One can easily foresee that any system based on filtering software invites gaming. At the most basic level, suspects could employ false keywords

---

90. *Id.* at 148 (Brennan, J., dissenting).

91. Kerr, *supra* note 12, at 578–79. Search procedures do not necessarily reveal intent. *Compare* United States v. Gray, 78 F. Supp. 2d 524, 530 (E.D. Va. 1999) (holding that examiner who opened directory marked "Tiny Teen" was not looking for child pornography but following routine search practice), *with* United States v. Carey, 172 F.3d 1268, 1273 (7th Cir. 1999) (holding that officer who admitted intent to locate child pornography deviated from initial search after finding first pornographic image).

92. *See Carey*, 172 F.3d at 1271.

93. *See id.* at 1277 (Baldock, J., concurring) ("In contrast, if the record showed that Detective Lewis had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, I think a different result would be required. That is not what happened here, however."); *see also* United States v. Burgess, 576 F.3d 1078, 1088–89, 1092 (10th Cir. 2009) (upholding admission of computer images of child pornography discovered during search for evidence of drug transport and stating that " the Carey holding was limited" and " fact intense").

94. *See, e.g.*, Kerr, *supra* note 12, at 579.

95. Using what Orin Kerr has referred to as a "perfect tool," law enforcement officers would be able to conduct tailored searches in the electronic world. *See* Kerr, *supra* note 12, at 579.

96. *See* Recent Case: CDT II, *supra* note 47, at 1009–10.

and forge timestamps to elude filters.[97] There are numerous examples of successful manipulation of metadata or file size.[98] In particular, the "responsive" approach is easily defeated. It is not difficult to structure files so that they will respond only to unique software.[99] Further, the greater move towards cloud computing means that computers may interact with content that cannot be viewed or opened locally. Professor Orin Kerr has succinctly debunked the arguments in favor of the technological approach:

> The problem with [the technological] approach is that it does not provide a judicially manageable standard. Dozens of different forensic programs exist, each with its own strengths, weaknesses, availability, and cost. The tools morph quickly over time, as do the latest techniques in hiding data. Which tool would be the best in any situation depends on how the officer was trained, how the tool was used, what techniques might have been used to try to thwart investigators, and what other tools were available at that particular time. Competing considerations such as cost and ease of use would also make it difficult for a court to require use of particular tools at any particular time.[100]

One could argue that, even if no technological tool could be completely successful, the implementation of the tool might capture the vast majority of offenders while keeping overly aggressive investigators at bay. Even if such a tool could be developed, it would require

---

97. Users of Napster employed this simple strategy with great success. Posting of Eliot Van Buskirk to Wired.com, Open Source 'Napster' Resurrected After 8-Year Dormancy, http://www.wired.com/epicenter/2009/11/open-source-napster-resurrected/ (Nov. 3, 2009, 13:03 PST).

98. *See, e.g.*, Bihari v. Gross, 119 F. Supp. 2d 309, 313–15 (S.D.N.Y. 2000) (manipulating metatags to direct Internet traffic); Mathias King, *A Critical Look at the Regulation of Computer Viruses*, 11 INT'L J.L. & INFO. TECH. 162, 165–67 (2003) (describing the various tools a computer virus may use to avoid detection).

99. An example of this trend would be the adoption of proprietary file types that can only be read on tethered devices. So while a computer may host a proprietary e-book, only a separate reader could utilize that e-book. *See* Dan Goodin, *Hackers Break Amazon's Kindle DRM*, THE REGISTER, Dec. 23, 2009, http://www.theregister.co.uk/2009/12/23/amazon_kindle_hacked/; Posting of Nilay Patel to Engadget, Kindle DRM Hacked To Allow Protected Mobipocket ebooks, http://www.engadget.com/2007/12/12/kindle-drm-hacked-to-allow-protected-mobipocket-ebooks/ (Dec. 12, 2007, 18:47 CST); Posting of David Rothman to TeleRead, Kindle Hack Lets You Read DRMed Mobipocket — and Meanwhile a 'Kindle Swindle' Tag Campaign Is Starting up, http://www.teleread.org/2007/12/12/kindle-swindle-tag-campaign-from-defectivebydesignorg/ (Dec. 12, 2007, 19:22 EST).

100. Kerr, *supra* note 12, at 579.

both continuous technological updates and courts savvy enough to recognize when these innovations are necessary and successful.

IV. A BETTER APPROACH: BALANCING SOCIETY'S INTEREST IN PREVENTING UNDERLYING CRIME AGAINST THE DEFENDANT'S INTEREST IN SEARCHED MATERIAL

The aforementioned approaches analogize digital searches to real world searches. The container approach conceptualizes a hard disk as a single physical object. The intent approach uses officer intent as a proxy for the scope of a warrant's physical coverage. The technological approaches attempt to restrict the scope of the search, not through physical boundaries, but by limiting a digital search to responsive data under the assumption that through technology we can discern information in the electronic context as naturally as we can in the physical world. These approaches fail because physical and electronic searches and seizures are fundamentally different. Instead of analogizing the physical to the electronic, we must craft a new doctrine, one that is more direct. This Part argues that a crime-based approach implemented through a judicial balancing test can accomplish the original goals of the plain view doctrine while both respecting a suspect's privacy rights and comporting with Rule 41 or *Horton*.

A. Balancing Test Best Serves Purposes of Plain View Doctrine

Before explaining the best approach to link the bounds of the search protocol to the crime alleged, it will be helpful to return to the principles that led to the plain view doctrine in the first place. It will become clear that the weight we accord to these principles ought to change when we consider their application in the digital domain.

The plain view doctrine accomplishes two main goals in the context of physical searches: (1) preventing the destruction of evidence and (2) protecting society from future harm.[101] A suspect who has witnessed a search of his property is likely to destroy any incriminating evidence outside of the scope of the warrant.[102] Further, evidence of other criminal acts signals a continuing danger to society. If officers delayed in acting on this information, additional crimes could be

101. *Cf.* Coolidge v. New Hampshire, 403 U.S. 443, 468 (1971) (holding that requiring a second warrant for plain view evidence would "be a needless inconvenience, and sometimes dangerous — to the evidence or to the police themselves").

102. *See* Segura v. United States, 468 U.S. 796, 800–01, 816 (1984) (describing procedures used to prevent the destruction of evidence and finding there is no constitutional right to destroy evidence); Cupp v. Murphy, 412 U.S. 291, 298–99 (1973) (discussing likelihood that suspect will destroy evidence when alerted to its existence); *see also* Chimel v. California, 395 U.S. 752, 762–63 (1969) (discussing need to prevent possible destruction or concealment of evidence by arrestee).

committed in the interim; alternatively, the police officers themselves may become victims of crime when they return to collect the incriminating evidence.[103]

The first concern does not exist in most digital searches because the government already possesses a stable, complete copy of the suspect's hard drive.[104] It is standard procedure for officers to first use a write blocker to prevent a suspect's hard drive from being altered or corrupted. Then, the officer captures an exact copy of the hard drive's data.[105] This copy is examined offsite, often months after the initial seizure.[106] In this way, data is seized or copied before they are searched, and the original hard drive may remain in the suspect's possession. Provided that law enforcement may retain a copy indefinitely, there is no worry that a defendant will wipe files from his own drive.

Instead, the danger to the public becomes the primary motivation for the use of the doctrine in digital searches. Accordingly, the use of the plain view doctrine in the digital context should hinge on the underlying danger of the crime implicated by the out-of-scope evidence. In determining if plain view digital evidence should be suppressed, the court should balance the interests of society against the defendant's justified expectation of privacy in the body of the searched material.

B. Applying the Balancing Test

The crime-based approach instructs courts to employ a balancing test ex post in order to determine if officers may use electronic evidence that is outside of the scope of the initial warrant. Under this approach, courts would weigh society's interest in preventing the underlying crime against the defendant's (and any third parties') justified privacy interest in the searched material.

It is important to note that no metric would allow precise weighing of each interest for all cases. Like all such rules, predictability and accuracy arise from repeated applications of the test, which through precedent, can reveal a loose hierarchy of crimes and contexts under each prong of the test. The following two Subparts provide specific examples of crimes that best illustrate how each prong ought to be

---

103. *Coolidge*, 403 U.S. at 468; *see also* Donald B. Allegro, Note, *Police Tactics, Drug Trafficking, and Gang Violence: Why the No-Knock Warrant is an Idea Whose Time has Come*, 64 NOTRE DAME L. REV. 552 (1989) (describing the threat that alerted suspects pose to officers).

104. Digital searches can occur months after the actual physical seizure of both the suspect and computer hardware. *See, e.g.*, United States v. Mann, 592 F.3d 779, 781 (7th Cir. 2010) (describing detective's digital search, occurring two months after defendant was arrested and investigators seized his digital media).

105. *See* Kerr, *supra* note 12, at 540–41, for a more detailed exploration of bitstreaming copying. For an example of this procedure, see *Mann*, 592 F.3d at 781.

106. *See, e.g.*, *Mann*, 592 F.3d at 781.

applied. Subpart IV.B.3 then applies the crime-based balancing test to previously decided cases.

1. Society's Interest in Preventing the Underlying Crime

In determining the danger of the underlying crime, a court should look to the direct impact of the crime on third parties as well as the vulnerability of those third parties.[107] Both the impact on and the vulnerability of third parties vary according to the type of crime and the classification of victims.

Society has an acute interest in protecting its members from bodily harm. Therefore, officers are able to confiscate dangerous contraband in order to defuse a possible threat.[108] Furthermore, society has a vital interest in protecting exceptionally vulnerable individuals, such as children. Crimes against children are considered especially reprehensible and typically merit enhanced punishment.[109]

On the other hand, society has a relatively minor interest in protecting its members from fairly solitary crimes such as drug possession, small-time individual income tax evasion, or illegal personal downloading of music or movies. When crimes neither directly impact third parties nor target especially vulnerable victims, the interest of society would not overcome an individual's reasonably justified privacy interest.

2. Individual Privacy Interest in Searched Material

Unlike the evaluation of society's interest, analysis under the privacy interest prong is subject to a fairly clear precedential guideline. To determine if a privacy interest is justified, the court will look to the Supreme Court's decision in *California v. Ciraolo*.[110] There, the Court laid out a two-part test to determine if a defendant has a "constitutionally protected reasonable expectation of privacy."[111] "[F]irst, has the

107. Secondary indicia of the seriousness of an offense might also include the typical length of imprisonment and the difficulty in correcting resulting damage caused by the crime.

108. *See* Coolidge v. New Hampshire, 403 U.S. 443, 472 & n.28 (1971).

109. *See* Kennedy v. Louisiana, 128 S. Ct. 2641, 2658 (2008) (acknowledging the serious physical and emotional damage suffered by a child-victim of a sexual assault). Until the 5-4 decision of *Kennedy*, Louisiana allowed capital punishment for the rape of a child under the age of 12. Georgia, Oklahoma, South Carolina, and Texas had similar statutes. GA. CODE ANN. §§ 16-6-1(a)(2)–(b) (2010) (rape of victim under 10); OKLA. STAT. ANN. tit. 21, § 843.5(k) (West 2010) (rape of victim under 14 where defendant has a prior conviction for sexual abuse of a person under 14); S.C. CODE ANN. § 16-3-655(C)(1) (2010) (rape of victim under 11 where defendant is repeat offender); H.B. 8, 2007 Leg., 80th Sess. (Tex. 2007) (same as Okalahoma).

110. 476 U.S. 207 (1986).

111. *Id.* at 211 (quoting Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?"[112] Even if the privacy interest is justified, the court must determine the strength of that interest. In order to assess this, a court may look to the defendant's or third party's identity interest in the material, to the manner in which the material was originally authored or acquired, and to the legal protections typically afforded to the material.[113]

Individuals may possess a nearly absolute privacy interest in their medical records. These records are typically kept in secure locations and may not be disclosed to the general public. Medical information is deeply personal, reflecting a person's sexual history, psychological state, and personal habits. The law recognizes the great importance of medical privacy by prohibiting government intrusion in the doctor-patient relationship[114] and by punishing individuals who willfully disclose medical data.[115]

In contrast, an individual's privacy interest in a personal photo album may be fairly weak. Even if an individual has taken reasonable measures to keep pictures private, there is no criminal prohibition on the third-party disclosure of these pictures. While it is conceivable that some types of photos might warrant extra protection, these typically involve materials produced in connection to other established privacy interests.[116]

---

112. *Ciraolo*, 476 U.S. at 211 (summarizing the two-part inquiry of *Katz*).

113. Each of these factors can help the court determine if "the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment." *Ciraolo*, 476 U.S. at 212 (quoting Oliver v. United States, 466 U.S. 170, 182–83 (1984)). Courts often consider the defendant's relationship to the observed object when assessing the legality of police surveillance. In *Commonwealth v. One 1985 Ford Thunderbird Automobile*, 624 N.E.2d 547, 550 (Mass. 1993) the court applied a four factor test to uphold aerial surveillance: (1) "whether the police had a lawful right to be where they were," (2) "whether the public had access to, or might be expected to be in, the area from which the surveillance was undertaken," (3) "the nature of the intrusion," and (4) "the character of the area (or object) which was the subject of the surveillance"; the court also noted that "'if there is some justification for concentrating a surveillance on a particular place, as opposed to random investigation to discover criminal activity, that factor is weighed in the balance and contributes to justification for the surveillance.'" *Id.* at 551 (quoting United States v. Allen, 633 F.2d 1282, 1290 (9th Cir. 1980)); *see also* State v. Bryant, 950 A.2d 467, 473–78 (Vt. 2008) (describing various approaches to determining expectation of privacy). The law recognizes some deeply personal and private relationships, and limits the State's use of information derived from those relationships. *See, e.g.*, FED. R. EVID. 501 (concerning privileges).

114. Though there is no physician-patient privilege at federal common law, the privilege exists in various forms at the state level. *See, e.g.*, S.D. CODIFIED LAWS §§ 19-13-6 to 19-13-11 (2010) (South Dakota's physician-patient privilege and psychotherapist-patient privilege). *See generally* Daniel W. Shuman, *The Origins of the Physician-Patient Privilege and Professional Secret*, 39 SW. L.J. 661 (1985).

115. *See* 42 U.S.C. § 1320d-6 (2006) (providing penalties for wrongful disclosure of individually identifiable health information).

116. *See, e.g.*, Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 168, 171–72 (2004) (denying request for release of death-scene photos of Vincent Foster due to the "well

3. Case Studies

Applying this balancing test to the facts of *CDT II* and *Runyan*[117] helps illustrate the intuitive suitability of a crime-based approach. *CDT II* features a crime posing a relatively low danger to society and involves defendants and third parties with extremely high, justified privacy interests in the seized material. Conversely, *Runyan* features a crime posing an extremely high danger to particularly vulnerable members of society and a defendant with a relatively low privacy interest.

Had the court in *CDT II* conducted a well-reasoned balancing test regarding the privacy interests of individuals and the interest of the State in protecting future victims, the result would have been the same. The crime in *CDT II*, steroid use, was not particularly dangerous and did not involve an interpersonal offense.[118] At the same time, the players had extremely strong, justified privacy interests in their confidential medical data. Players took clear steps to keep the results of their steroid tests private. Further, both the law and society afford medical records an extraordinary level of protection.[119] Finally, the concerns raised in *CDT II* focus on the issue of third party privacy rights, an issue that is especially acute in the medical context.

Runyan presents the opposite picture, with a particularly dangerous crime and a weak privacy interest. There, the crime of producing and possessing child pornography implicated the State's powerful interest in protecting children and preventing the continued dissemination of such materials. In light of the many additional restrictions society imposes on sex offenders both in the courtroom[120] and after release[121] with the goal of protecting children, courts would not likely be willing to grant additional protections to individuals employing digital tools in a predatory manner. Furthermore, Runyan did not have a strong privacy interest in the materials. Though Runyan had taken

established tradition acknowledging a family's control over the body and death images of the deceased"); 45 CFR § 164.514 (2003) (prohibiting the disclosure of protected health information including "[f]ull face photographic images and any comparable images").

117. United States v. Runyan, 275 F.3d 449 (5th Cir. 2001).

118. *See supra* Part II.A.

119. *See, e.g.*, Health Insurance Portability and Accountability Act ("HIPAA"), Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033 (1996) (codified in scattered sections of 26, 29, and 42 U.S.C.).

120. *See, e.g.*, FED. R. EVID. 414 (creating exception allowing the introduction of "evidence of the defendant's commission of another offense or offenses of child molestation").

121. *See, e.g.*, United States v. Thielemann, 575 F.3d 265, 278 (3d Cir. 2009) (upholding release condition stripping sex offender of Internet access in order to protect the public); United States v. Paul, 274 F.3d 155, 170–72 (5th Cir. 2001) (restraining sex offender from access to photographic and audio-video equipment); *see also* Recent Case, United States v. Thielemann, *575 F.3d 265 (3d Cir. 2009)*, 123 HARV. L. REV. 776, 778, 781 (2010) (summarizing circuit approaches to Internet prohibitions in light of state motivation to protect children).

some steps to hide these materials from view, he did not encrypt or password-protect them. Additionally, Runyan did not have a strong identity interest in the materials; they consisted of photos he took of an underage neighbor. The privacy of the third party portrayed in the photograph was not an issue because the third party was a victim of the crime.[122]

C. Comporting with Rule 41 and Horton

The previous attempts to restrain electronic plain view, either through an outright ban on the practice or through an intent-based approach, have ignored the Supreme Court's preferences as expressed in Rule 41 and *Horton*. However, an approach that allows the alleged crime to form the parameters of the search would contradict neither of the Supreme Court's directives; it would allow the direct copying of a suspect's digital media while disregarding the investigating officer's subjective intent.

Rule 41 mainly serves as a codification of the common seizure practice wherein an officer copies all of a suspect's data, transports that copy to a lab offsite, and searches that data at a later date. To that end, Rule 41 states that a "warrant . . . may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information" and, unless otherwise noted, a "warrant authorizes a later review of the media or information."[123] An officer's inventory of electronic data may be "limited to describing the physical storage media that were seized or copied."[124] Finally, that "officer may retain a copy of the electronically stored information that was seized or copied."[125] All of these rules allow wide leeway in the copying and seizing of large amounts of data.

The crime-based approach would not interfere with this practice; officers may continue to copy the entirety of a suspect's data. However, the officer would be prohibited from acting on information derived from that data if the suspect's justified privacy interest in the searched material outweighs society's interest in preventing the underlying crime. This approach does not require the court to determine the investigating officer's subjective state of mind, as forbidden by

122. Even supposing that Runyan's computer contained private correspondence with parties other than his victim, this material is not afforded the same amount of protection as medical data. *See* HIPAA, *supra* note 119. Furthermore, in the context of child exploitation, the correspondence of the defendant is often a crime in and of itself. *See, e.g.*, *Thielemann*, 575 F.3d at 275–77.

123. FED. R. CRIM. P. 41(e)(2)(B).

124. FED. R. CRIM. P. 41(f)(1)(B).

125. *Id.*

Horton.[126] Instead, the approach squarely focuses on the interests of the involved parties, individuals with connections to the searched data and the state itself.

D. Preserving Case Outcomes While Formulating a Coherent Standard

When courts adopt new approaches, they do so like the sailors in Otto Neurath's boat, "who have to rebuild their ship on the open sea, without ever being able to dismantle it in dry dock and reconstruct it from the best components."[127] One additional benefit of the balancing approach is that its adoption would not work a significant change on existing law.

The application of the proposed crime-based balancing test for plain view would return many of the same outcomes as current approaches while also providing a versatile safeguard for both defendants and the public generally. The Ninth Circuit could embrace caution in the medical context under a balancing test and, in so doing, avoid a blanket rule that would obstruct and encumber cases regarding exploited children.[128] The Fifth Circuit could allow police officers to conduct thorough examinations of hard disks containing child pornography without relying on a false comparison of computers to cabinets.[129] Accordingly, a crime-based approach would not disrupt the underlying case law in a contentious field and would allow courts to conduct more comprehensible analyses in a murky area.

Courts applying a balancing test that weighs the danger of the underlying crime against the privacy interest of the defendant could realize the socially beneficial results of other digital search approaches without conflating the physical and the electronic. The test would suppress the incriminating evidence in *CDT II* and would not suppress the incriminating evidence in cases such as *Runyan*.

E. Avoiding a Statutory Definition

The aforementioned balancing test offers a promising adaptation of the plain view doctrine. However, some might argue that this approach sacrifices the efficiency of a bright-line legal rule.[130] The legis-

126. Horton v. California, 496 U.S. 128, 140 (1980) ("[N]o additional Fourth Amendment interest is furthered by requiring that the discovery of [plain view] evidence be inadvertent.").

127. Otto Neurath, *Protocol Statements*, *in* PHILOSOPHICAL PAPERS 1913–1946 92 (Robert S. Cohen & Marie Neurath eds. & trans., 1983).

128. *See supra* Part IV.B.3.

129. *See id.*

130. *See generally* Kathleen M. Sullivan, The Supreme Court 1991 Term: Foreword: *The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 58 (1992) (defining a rule as "[a] legal directive . . . [that] binds a decisionmaker to respond in a determinate way to the pres-

lature could provide a statutory definition of per se dangerous offenses that authorize the use of plain view digital evidence. This approach is certainly not novel; Congress used a similar technique to qualify the use of federal wiretapping in the Wiretap Act.[131] Child molestation and crimes related to terrorism likely would be among the first offenses on this list of triggering categories.[132] However, this approach would cause some concern because the legislature has little incentive to constrain the list of per se dangerous offenses.[133] Again, the Wiretap Act can serve as a useful case study.[134] The Act originally restricted the use of wiretaps to a small number of federal crimes.[135] However, Congress repeatedly expanded the number of triggering offenses so that the Act now includes "essentially every federal felony offense that is prosecuted with any regularity."[136]

V. CONCLUSION

The application of the plain view doctrine to the digital world continues to perplex courts. The Ninth Circuit's attempts to do away with the doctrine will have little impact in light of Rule 41. Unfortunately, Rule 41 fails to ease the greater confusion of applying a real

---

ence of delimited triggering facts. Rules aim to confine the decisionmaker to facts, leaving irreducibly arbitrary and subjective value choices to be worked out elsewhere . . . ." (citations omitted)). Sullivan further explains that:

> A legal directive is "standard"-like when it tends to collapse decisionmaking back into the direct application of the background principle or policy to a fact situation. Standards . . . [give] the decisionmaker more discretion than do rules. Standards allow the decisionmaker to take into account all relevant factors or the totality of the circumstances. Thus, the application of a standard in one case ties the decisionmaker's hand in the next case less than does a rule - the more facts one may take into account, the more likely that some of them will be different the next time.

Id. at 58–59 (citations omitted); *see also* Brian Sheppard & Fiery Cushman, *Evaluating Norms: An Empirical Analysis of the Relationship Between Norm-Content, Operator, and Charitable Behavior*, 63 VAND. L. REV. 55, 58–68 (2010) (discussing characteristics of and preconceptions regarding rules and standards).

131. 18 U.S.C. §§ 2510–2522 (2006).

132. *See* Kerr, *supra* note 12, at 580 (suggesting that this approach "[p]erhaps . . . could be used only in terrorism cases, or perhaps only in terrorism cases, homicide cases, and child pornography cases").

133. The constant campaigning for re-election forces members of Congress to focus on advertising, credit claiming, and position taking. *See* DAVID R. MAYHEW, CONGRESS: THE ELECTORAL CONNECTION 49–55, 60–62, 130–36 (2d. ed. 2004). No member would willingly advertise a "soft on crime" stance, nor claim credit for a bill stating the same. Demanding high criminal sentences is often a path to political success. The Economist, Prosecutor or Politician?, http://www.economist.com/blogs/democracyinamerica/2010/01/prosecutor_or_politician (Jan 13, 2010 23:02 EST).

134. *See* JEFFREY ROSEN, THE UNWANTED GAZE 37 (2001) (discussing the expansion in the list of crimes justifying government wiretapping); Kerr, *supra* note 12 at 581.

135. Kerr, *supra* note 12 at 581.

136. *Id.*

world doctrine to the digital context. Other approaches to the problem, such as the intent test of *Carey* and the imagined "perfect tool," also do not provide a practical solution. By implementing an ex post judicial balancing test weighing society's interest in protection against a defendant's interest in the privacy of the material searched, courts may render suppression judgments more consistently and honestly.