What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine

"The shift from physical evidence to digital evidence often leads to a shift in how investigators collect evidence; changes in how evidence is collected leads to pressure for new legal rules to regulate evidence collection. The warrant process is merely one part of a broader mosaic of the mechanisms of the investigative process that will be reformed."[1]

I. INTRODUCTION

The development of digital technology has created a unique set of problems for courts attempting to determine whether certain practices pertaining to search and seizure of digital forensic evidence are violative of the Fourth Amendment.[2] The significant inherent differences between physical and digital property make a traditional application of the Fourth Amendment ill-fitting and unworkable.[3] Congress and the courts have attempted to grapple with the doctrinal inconsistencies that result from the physical-digital distinction by recognizing modifications in the practices, policies, and procedures that govern the search and seizure of digital evidence.[4] In the absence of well-defined

1. Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 134 (2005).

2. *See* Lily R. Robinton, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311, 323 (2010) (indicating extensive use and storage capacity of digital media complicates digital searches).

3. *See* Kerr, *supra* note 1, at 86-87 (advocating warrant process needs reform to accommodate digital evidence); *see also* Bryan K. Weir, Article, *It's (Not So) Plain to See: The Circuit Split on the Plain View Doctrine in Digital Searches*, 21 GEO. MASON U. C.R. L.J. 83, 85 (2010) (discussing difficulty of applying Fourth Amendment doctrine to digital evidence).

4. *See* FED. R. CRIM. P. 41(e)(2) advisory committee's notes to 2009 amendments (amended 2011) (acknowledging digital searches require bifurcation of warrant execution given unique characteristics); *see also* Kerr, *supra* note 1, at 115-24 (discussing various decisions grappling with searches and seizures of digital media); Robinton, *supra* note 2, at 323-24 (providing cases evaluating Fourth Amendment in digital context); Derek Haynes, Comments, *Search Protocols: Establishing the Protections Mandated by the Fourth Amendment Against Unreasonable Searches and Seizures in the World of Electronic Evidence*, 40 MCGEORGE L. REV. 757, 765 (2009) (opining procedures to obtain physical information inadequate for electronic information); Weir, *supra* note 3, at 90-105 (summarizing various circuits' approaches to deciding search-warrant cases in digital context). "[T]he Supreme Court, Congress, prominent judges, lawyers, and law professors have all agreed that the procedures governing physical information are simply inadequate when applied to electronic information. As a result, the Advisory Committee on the Federal Rules of Civil Procedure amended the rules . . . to account for these insufficiencies." Haynes, *supra*, at 765.

rules, however, courts are implementing widely varied and inconsistent approaches to determine whether the government violated the timing and particularity requirements of search warrants under the Fourth Amendment.[5]

In 2009, Congress codified one doctrinal modification by amending Rule 41 of the Federal Rules of Criminal Procedure to permit the government to investigate the contents of media seized after the physical execution of the warrant.[6] Prior to its amendment, Rule 41(e)(2)(A)(i) required that a warrant be executed within a specified period no longer than fourteen days from the date of issuance, as determined by a magistrate.[7] This rule created confusion among the courts concerning whether the execution deadline pertained only to physical evidence, or whether the forensic examination had to be conducted within that timeframe as well.[8] By amending the rule, Congress recognized that applying the standards of a physical search and seizure to a digital search and seizure is unreasonable and unworkable.[9] Despite this recognition,

5. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc. (*CDT III*), 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (holding plain view doctrine inapplicable in digital context); United States v. Mann, 592 F.3d 779, 785-86 (7th Cir. 2010) (determining files discovered within hard-drive reasonably extended from sufficiently particularized warrant); United States v. Mutschelknaus, 592 F.3d 826, 829-30 (8th Cir. 2010) (reconciling Rule 41 and magistrate-granted extension of execution); United States v. Syphers, 426 F.3d 461, 469 (1st Cir. 2005) (balancing reasonableness of delay against forensic lab backlog in determining constitutionality); United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (suggesting particularity requirement in computer searches depends on facts of each case); United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (indicating constitutionality of subsequent off-site computer examinations when warrant execution timely).

6. *See* FED. R. CRIM. P. 41(e)(2)(B) (amended 2011) (amending rule in 2009 to clarify timing requirements for digital searches).

7. FED. R. CRIM. P. 41(e)(2)(A)(i) (amended 2011) (providing officer must "execute the warrant within a specified time no longer than 14 days").

8. *See* Kerr, *supra* note 1, at 115-23 (discussing attempts to resolve timing question for digital warrants).

9. *See* FED. R. CRIM. P. 41(e)(2)(B) (amended 2011) (amending rule in 2009 to exclude digital searches from timing deadline). The amended rule states:

> 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.

Id. Courts generally recognized that to require the police to search a defendant's computer at his or her home during the time of search and seizure would create an impractical and burdensome protocol. *See, e.g.*, Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (noting "obvious difficulties attendant in separating the contents . . . from the computer hardware during . . . a search"); United States v. Schandl, 947 F.2d 462, 465-66 (11th Cir. 1991) (suggesting greater disruption if "thorough search of each . . . document and computer disc before removing it"); United States v. Henson, 848 F.2d 1374, 1383-84 (6th Cir. 1988) (determining unreasonable to require officers to sift through documents and computer files on scene); *see also* Kerr, *supra* note 1, at 129-30 (recognizing different timing needs for digital evidence and suggesting amendment of warrant rules); Robinton, *supra* note 2, at 324-25 (highlighting impracticality of treating timing for digital and physical evidence in same manner). *But see* United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006) (requiring magistrate approval to "seize the haystack to look for the needle").

Congress provided no guidance as to the appropriate end date by which forensic examiners must conduct their search, which has resulted in disparate decisions by the courts.[10]

Additionally, the Advisory Committee Notes on the 2009 amendments to Rule 41(e)(2) indicate that Congress intentionally refused to address the particularity with which one must describe the digital evidence sought in the warrant and left the issue to be settled by the courts.[11] Without a rule specifying the degree of particularity required to obtain a warrant, the courts have struggled to reconcile the plain view doctrine in the digital context where the forensic examiner discovers previously unknown, incriminating evidence that was not particularized in the warrant, and for which there was no probable cause to seize.[12] Under the traditional application of the plain view doctrine to physical property, evidence can be seized and used to prosecute the defendant so long as it is clearly located in plain view and the investigator had lawful right of access to it.[13] For example, if the examiner finds incriminating evidence in the process of opening files, the plain view doctrine holds that the evidence could potentially be lawfully seized, regardless of its relation to the original warrant.[14] Absent guidance from Congress or the Supreme Court, it is unclear what degree of particularity is required for executing a warrant.[15] As a result, the circuit courts are split as to how, and in what capacity, the plain view doctrine should be applied to digital evidence.[16]

10. *Compare* United States v. Grimmett, No. 04-40005-01-RDR, 2004 WL 3171788, at *5 (D. Kan. Aug. 10, 2004) (holding ninety-six hours reasonable for search), *with Syphers*, 426 F.3d at 469 (holding five-month delay of search reasonable).

11. *See* FED. R. CRIM. P. 41(e)(2) advisory committee's notes to 2009 amendments (amended 2011). The advisory committee notes provide: "The amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development." *Id.*

12. *See* James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 FORDHAM L. REV. 2809, 2829-30 (2011) (examining courts' struggle to apply plain view doctrine in digital context); *see also* Andrew Vahid Moshirnia, Note, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J.L. & TECH. 609, 612-13 (2010) (highlighting difficulty of reconciling plain view doctrine with narrowly tailored warrants).

13. *See* Horton v. California, 496 U.S. 128, 136-37 (1990) (outlining plain view doctrine three-prong test); *see also* Saylor, *supra* note 12, at 2820-22 (summarizing origins and requirements of plain view doctrine); Weir, *supra* note 3, at 83-84 (providing summary of plain view doctrine).

14. *See* Robinton, *supra* note 2, at 333 (noting digital application of plain view doctrine allows search of evidence not covered in warrant); *see also* Saylor, *supra* note 12, at 2829 (suggesting "brief perusal" of documents in digital search intrusively allows access to plain view doctrine).

15. *See* FED. R. CRIM. P. 41(e) advisory committee's notes to 2009 amendments (amended 2011) (noting absence of particularity requirement in warrant for electronically stored data).

16. *See CDT III*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (determining traditional plain view doctrine not applicable to digital evidence); United States v. Mann, 592 F.3d 779, 785-86 (7th Cir. 2010) (opining plain view doctrine should progress incrementally); United States v. Williams, 592 F.3d 511, 521-22 (4th Cir. 2010) (holding traditional plain view doctrine applies to digital evidence); United States v. Carey, 172

This Note will analyze the timing and particularity issues left unresolved by Congress's 2009 amendment to Rule 41.[17] Part II.A will provide a history of the case law, highlighting the ambiguity surrounding the timeline requirements of Rule 41(e)(2)(B).[18] Part II.B will discuss how the lack of a particularity rule has forced the courts to confront the plain view doctrine's application to digital evidence.[19] Part II.B will also examine the approaches that various circuit courts have taken to address this issue.[20] Part III will analyze the cases outlined in Parts II.A and II.B, as well as the various approaches courts have taken to address timing and the plain view doctrine's application to digital evidence.[21] In addition, Part III will discuss how Congress's failure to resolve these issues in its 2009 amendment is problematic for both defendants and examiners, as well as for judicial efficacy and the interests of justice.[22] Finally, this Note will propose amending Rule 41 to better serve defendants, examiners, and the judicial process.[23]

II. HISTORY

A. The Road to the Amendment

1. Pre-2009 Amendment

In 2009, Congress amended the Federal Rules of Criminal Procedure in an effort to clarify Rule 41(e), which governs the procedure for issuing a search warrant.[24] Prior to the amendment, Rule 41 stated that a search warrant must be executed within a specified period of time, no longer than ten days.[25] Attempts by magistrates to authorize warrants for digital evidence under this rubric exposed inconsistencies between the search and seizure procedures of traditional physical evidence and digital evidence.[26] Specifically, the search

F.3d 1268, 1274-76 (10th Cir. 1999) (indicating plain view analysis fact driven, but cautioning officers cannot conduct sweeping comprehensive search).

17. *See infra* Parts II-IV (analyzing unresolved issues of Rule 41 amendment).

18. *See infra* Part II.A (summarizing timeline requirement ambiguity in Rule 41 case law).

19. *See infra* Part II.B (discussing effects of lack of particularity rule).

20. *See infra* Part II.B (examining circuit court approaches).

21. *See infra* Part III (outlining various approaches to timing and plain view doctrine's application to digital evidence).

22. *See infra* Part III (addressing judicial impact of failure to resolve issues).

23. *See infra* Part IV (suggesting Rule 41 amendment).

24. *See* FED. R. CRIM. P. 41(e) (amended 2011) (governing to whom warrant may be issued and its contents).

25. *See* FED. R. CRIM. P. 41(e)(2)(a) (amended 2011) (providing time requirement for execution of search warrant); *see also* Kerr, *supra* note 1, at 129-32 (discussing ambiguity of applying unamended Rule 41(e) to search and seizure of digital evidence). In addition to the ten-day execution requirement, Rule 41(e) stated that a search warrant must command the officer to "execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time." *See* FED. R. CRIM. P. 41(e)(2)(b)(ii) (amended 2011).

26. *See In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) (noting difficulties

and seizure of digital evidence requires that the police take an additional step when executing the warrant: Once they have lawfully searched the premises and seized the evidence specified in the warrant, they must subsequently search the seized evidence for indicia of the criminal activity that supported authorization for the warrant.[27] While the time limit prescribed by the unamended rules provided a reasonable balance between police exigencies and an accused's privacy concerns with regard to search and seizure of physical property, search and seizure of digital evidence required a different analysis of reasonableness given concerns arising out of digital searches.[28]

Various court decisions attempting to apply Rule 41 to digital evidence exposed such inconsistencies where police were unable to execute the warrant within the ten-day limit prescribed by the rule.[29] Absent bright-line guidance, the courts employed various methods of distinguishing the facts of each case and rarely declared a search unreasonable despite its not being executed within the ten-day requirement.[30] In one such case, *United States v. Syphers*, the court

of on-site computer searches off site and accompanying additional authorization); *see also* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 82 (2002) (proffering digital searches require additional content search subsequent to search of premises); Kerr, *supra* note 1, at 85-87 (suggesting differences in search and seizure of digital versus physical evidence require different rule-handling). In *West End*, the court acknowledged the inherent discrepancies in the two procedures and stated that "it is frequently the case with computers that the normal sequence of 'search' and then selective 'seizure' is turned on its head. Because of the difficulties of conducting an on-site search of computers, the government frequently seeks . . . authority to seize computers without any prior review of their contents." *See W. End*, 321 F. Supp. 2d at 958. Acknowledgement of these differences in large part promulgated the amendment to the rule. *See supra* note 9 and accompanying text (discussing catalysts for amendment).

27. *See* Kerr, *supra* note 1, at 86 (suggesting bifurcated approach to digital search and seizure procedure better accounts for technological differences). *But see* David J.S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 841-42 (2005) (arguing amending warrant rules unnecessary despite expansive role and novel issues presented by computers). The rules governing search-warrant procedure were premised upon a one-step process whereby police obtained a warrant to enter the location to be searched, and then seized any property named in the warrant. *See* Kerr, *supra* note 1, at 86. Contrastingly, the search and seizure of digital evidence is premised upon a two-step process: The police first execute the physical search of the premises, seize the computer or digital storage device, and then subsequently search the device. *See id.*

28. *See* Kerr, *supra* note 1, at 130 (enumerating various concerns arising out of digital searches not present in physical searches). To comply with Rule 41(e) prior to its amendment, police or forensic examiners attempting to search a seized computer were forced to either process a vast amount of digital information within ten days, or hope that a magistrate would grant an extension for the warrant. *See id.* at 129. The ten-day time limit proved especially problematic given the common occurrence of backlogs and delays in government forensic laboratories, which are often not the forensic examiner's fault. *See id.*

29. *See* United States v. Syphers, 426 F.3d 461, 469 (1st Cir. 2005) (determining five-month delay in execution of warrant reasonable); United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (deciding two-month delay in execution reasonable despite failure to petition for extension); State v. Zinck, No. 03-S-1000-1024, 04-S-2393-2444, 2005 WL 551447, at *4 (N.H. Super. Ct. Feb. 4, 2005) (finding eighteen-month lapse between warrant's authorization and execution unreasonable); *see also* United States v. Habershaw, No. CR. 01-10195-PBS, 2002 WL 33003434, at *8 (D. Mass. May 13, 2002) (rejecting claim subsequent off-premises computer search constitutes second execution of warrant).

30. *See, e.g.*, *Syphers*, 426 F.3d at 468 (holding ten-day stricture not applicable in state investigation

indicated that a warrant extending the time limit for execution may be overbroad, yet still reasonable, as long as the delay does not unduly prejudice the defendant.[31] In *United States v. Triumph Capital Group*, the court applied the Federal Rules, but minimized the weight of their application, stating that "[t]he requirements of Rule 41 are basically ministerial in nature and violations of the rule only require suppression where the defendant is legally prejudiced."[32] Deviating even further from the ten-day requirement in Rule 41, the court in *United States v. Hernandez* found that the Federal Rules of Criminal Procedure do not supply a specific time limit in which a computer must undergo forensic examination; rather, if the police seize the data authorized by the search warrant in the time frame established by the magistrate, the actual examination of the data may take a substantial, unspecified period of time.[33] Conversely, the court in *State v. Zinck* applied the reasoning in *Hernandez*, but distinguished it by determining that the extensive time delay was unreasonable and violated the defendant's Fourth Amendment rights.[34]

absent federal agent participation); United States v. Triumph Capital Grp., 211 F.R.D. 31, 66 (D. Conn. 2002) (maintaining delay in execution not unreasonable unless probable cause no longer exists); *Hernandez*, 183 F. Supp. 2d at 480 (reasoning data seized but not examined within ten days not violative or unconstitutional).

31. *See Syphers*, 426 F.3d at 469 (holding delay in execution does not invalidate search if no undue prejudice); *see also* Kerr, supra note 1, at 120 (summarizing holding in *Syphers*). Despite its determination that the investigation was not federal in character—such that the strict ten-day deadline under the federal rules was inapplicable—the court determined that a seven-month extension was reasonable by evaluating the policy behind the ten-day requirement in the rule, including legitimate practical law-enforcement needs. *See Syphers*, 426 F.3d at 468-69. The court held that where the rationale of the rule prevents execution of stale warrants, a delay in execution does not render seized evidence inadmissible "absent a showing of prejudice to the defendants resulting from the delay." *Id.* at 469. The court circumvented applying Rule 41 by evaluating such traditional Fourth Amendment concerns as undue delay, lapse in probable cause, and bad faith, and suggested that excessive delay in the forensic process may make the search unreasonable. *See id.* at 468-69.

32. *See Triumph*, 211 F.R.D. at 65. Recognizing the difficulty of applying a ten-day execution requirement to digital evidence when the rule was designed for physical evidence, the *Triumph* court stated that "computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution." *Id.* at 66. The court instead determined reasonableness of the search by evaluating whether or not probable cause had gone stale. *See id.*; *see also In re* Search of Scranton Hous. Auth., 436 F. Supp. 2d 714, 727-28 (M.D. Pa. 2006), *vacated*, 487 F. Supp. 2d 530 (M.D. Pa. 2007) (adopting staleness approach discussed in *Triumph* and *Ellis*); Commonwealth v. Ellis, Nos. 97-192, 97-193, 97-563, 97-562, 97-561, 98-355, 97-356, 1999 WL 823741, at *28 (Mass. Super. Ct. Aug. 18, 1999) (proffering reasonable time for execution of digital searches largely dependent on computer-specific factors).

33. *See Hernandez*, 183 F. Supp. 2d at 480. The *Hernandez* court further found that so long as data was seized within the time limit specified in the warrant, the government need not apply for an extension or additional warrant if the search of data occurred later than the time designated in the warrant for search. *See id. But see Zinck*, 2005 WL 551447, at *4. In *Zinck*, the court rejected the ruling in *Hernandez*, deciding that the eighteen months it took for the government to forensically analyze the defendant's computer was an unreasonable delay in execution. *See id.* Although the facts presented in *Zinck* were similar to those in *Hernandez*, the *Zinck* court found the government's delayed forensic examination to be per se unreasonable. *See id.* at *2-3.

34. *See Zinck*, 2005 WL 551447, at *2-3. Despite noting that the state forensic lab was backlogged, and that only one technician was available to perform the search, the court found that the defendant bore the burden

2. Rule 41(e) Amended

Given the ambiguity resulting from the time limit component of Rule 41(e)(2)(a) and its application to computer searches, Congress amended the rule to specifically exclude computer and electronic media searches from the ten-day deadline.[35] The comment to the amendment suggests that the revised rule is designed to account for unique differences between physical and digital evidence.[36] Noting that computers and other electronic-storage media often contain enormous amounts of information, making it impractical for law enforcement to search and review it all during the execution of the warrant at the search location, the comment reflects that digital searches occur in a two-step process.[37] Additionally, rather than try to delineate a specific time period in which a computer search must be executed, Congress acknowledged "the practical reality is that there is no basis for a 'one size fits all' presumptive period," and prescribed a fourteen-day period for the actual execution of the warrant and onsite activity, but left the time allotted for search of the digital media unspecified.[38] As such, the statutory rules only regulate the timing of the government's physical search of the premises specified in the warrant, but do not regulate the timing of the digital-search stage.[39]

---

of these "resource deficiencies" when forced to wait eighteen months for the search to be executed. *See id.*

35. *See* FED. R. CRIM. P. 41(e) advisory committee's notes to 2009 amendments (amended 2011); *see also infra* Part II.B (discussing courts' difficulty in applying rule). In addition to extending the time period that police may execute a warrant from ten days to fourteen, the rule was amended to include a subsection that specifically addresses warrants seeking electronically stored information. *See* FED. R. CRIM. P. 41(e)(2)(B) (amended 2011). The amended rule specifically authorizes the seizure of electronic-storage media or information stored electronically, and provides that "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." *Id.*

36. *See* FED. R. CRIM. P. 41(e) advisory committee's notes to 2009 amendments (amended 2011) (addressing issue of electronically stored information). Unlike physical property subject to a warrant, the comment notes that computers and other forms of electronic-storage media often contain immense amounts of information, such that an on-site forensic examination would be impractical. *See id.*; *see also* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1250 (2010) (suggesting seizure and subsequent off-site search of digital evidence as practical approach).

37. *See* FED. R. CRIM. P. 41(e) advisory committee's notes to 2009 amendments (amended 2011). The notes to the amendment provide that "[t]his rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." *Id.* This alters the existing presumption that an investigator could enter the dwelling to be searched, seize property that was named in the warrant, and then leave having fully executed the warrant. *See* Kerr, *supra* note 1, at 86.

38. FED. R. CRIM. P. 41(e) advisory committee's notes to 2009 amendments (amended 2011). In coming to this determination, Congress accounted for substantial time that may be required to forensically image and review information stored on a computer. *See id.* Because of the sheer size of digital media's storage capacity, the difficulties that might arise with encryption and decoding, and the workload that many government forensic labs are faced with, digital searches may require a substantial, yet unpredictable, amount of time to complete. *See id.* Although the advisory notes provide that a judge may impose a deadline for access to the electronically stored information, or a return of the storage media, arbitrarily setting a deadline for return may result in frequent petitions to the court for additional time. *See id.*

39. *See id.*; *see also* Kerr, *supra* note 36, at 1251 (noting absence of statutory rule regulating electronic stage of computer searches). The federal rules explicitly provide that the "time for executing the warrant . . .

Although the amendment to Rule 41 clarified the extent to which the execution deadline applied to digital searches, it also created a new point of ambiguity for the courts to grapple with: What, if any, limitation exists on the timing of the digital-search stage of the computer warrant?[40] In omitting a time frame for the completion of digital searches, the Federal Rules provide very little guidance to the magistrates issuing the warrants, the law enforcement agents conducting the searches, and the judges determining whether evidence derived from the searches should be admitted or suppressed.[41] This ambiguity has resulted in a lack of cohesion amongst the courts in how to address the temporal scope of electronic searches.[42]

In some instances, courts have indicated that the Fourth Amendment—although lacking an explicit deadline—may be the source of restriction governing the timing of digital searches.[43] For example, in *United States v. Mutschelknaus*, law enforcement officials executed the physical search and seizure of evidence at the location listed in the warrant within ten days, and then subsequently forensically examined the computer equipment seized during the search within sixty days.[44] Absent an express timing restriction in Rule 41, the court looked to constitutional considerations, such as prejudice to the defendant and reckless disregard for proper procedure, to evaluate whether a sixty-day delay in executing the computer-search stage of the warrant was permissible.[45] Observing no evidence that the police manifested bad faith, or

refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." *See* FED. R. CRIM. P. 41(e)(2)(B) (amended 2011); *see also* Kerr, *supra* note 36, at 1251 (noting distinction).

40. *See* Kerr, *supra* note 36, at 1251 (acknowledging unresolved ambiguity resulting from Rule 41(e)(2)(B) amendment).

41. *See* Kerr, *supra* note 1, at 86 (suggesting federal rules provide adequate guidance in physical but not digital context).

42. *See* Kerr, *supra* note 36, at 1252-55 (citing various decisions that employ diverse approaches to rectifying statutory temporal ambiguity); *see infra* notes 43-64 and accompanying text (discussing various cases attempting to resolve timing ambiguity associated with Rule 41(e) and digital evidence).

43. *See, e.g.*, United States v. Mutschelknaus, 592 F.3d 826, 830 (8th Cir. 2010) (considering prejudice to defendant and reckless disregard for procedure in timing restrictions); United States v. Brewer, 588 F.3d 1165, 1173 (8th Cir. 2009) (holding delay in execution not unconstitutional where probable cause determination unaffected); United States v. Syphers, 426 F.3d 461, 468-69 (1st Cir. 2005) (declaring federal rules inapplicable; applying Fourth Amendment reasonableness rubric instead); *see also* Kerr, *supra* note 36, at 1251 (suggesting courts have hinted at existence of Fourth Amendment time restriction for digital searches). *But see* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.7(a) (4th ed. 2004 & Supp. 2012) (suggesting no constitutional, statutory, or rule-based requirements governing electronic stage of computer searches).

44. *See Mutschelknaus,* 592 F.3d at 828 (providing facts of case).

45. *See id.* Looking at *Syphers* and *Spencer* for guidance, the court reasoned that even if Rule 41 was violated, it does not automatically render evidence inadmissible. *See id.* at 829; *see also* United States v. Spencer, 439 F.3d 905, 913 (8th Cir. 2006) (suggesting Fourth Amendment, not Rule 41, supplies temporal boundaries); *Syphers*, 426 F.3d at 469 (applying Fourth Amendment considerations to delay analysis). Rather, the court noted that the defendant did not allege prejudice, and that the officer, in soliciting additional time to perform the forensic examination, acknowledged that computer examinations may take a considerable amount

that the defendant suffered undue prejudice, the court denied the motion to suppress.[46]

Also suggesting that the Fourth Amendment may provide temporal restrictions on how long law enforcement has to conduct the computer-search stage of a warrant's execution, the court in *United States v. Brewer* determined that whether the execution of the forensic analysis is timely turns on whether the delay in execution renders the warrant stale.[47] The defendant in *Brewer* argued that according to state law, a search warrant expires if not executed within ten days; thus, because the forensic analysis of his computer was conducted after ten days, it constituted a warrantless search in violation of his Fourth Amendment rights.[48] Adopting the reasoning employed in *Syphers*, the court evaluated the timeliness of the warrant's execution under the Fourth Amendment's "unreasonable delay" standard, rather than under the ten-day limit as prescribed by state law.[49] Upon determining that the constitutional and rule-embodied policies at issue were designed to ensure that a warrant had not gone stale, the court determined that based on the nature of the evidence at issue, the delay in searching the electronic media had no effect on probable cause.[50]

While in the above-mentioned cases the Fourth Amendment served as the limiting point for what constituted a reasonable delay in executing the search component of the warrant, in other cases the magistrates issuing the warrants have attempted to impose ex ante restrictions on the timing of electronic searches by providing law enforcement with a specified period to conduct the forensic examination.[51] In *United States v. Brunette*, the magistrate issuing the

of time. *See Mutschelknaus*, 592 F.3d at 829. Accordingly, the court found that irrespective of Rule 41, no constitutional considerations were implicated that would require suppression of the evidence. *See id.*

46. *Mutschelknaus*, 592 F.3d at 830.

47. *See Brewer,* 588 F.3d at 1173 (holding constitutional and rule-based policies designed to prevent execution of stale warrants).

48. *See id.* at 1172 (setting forth defendant's argument).

49. *See* United States v. Brewer, 588 F.3d 1165, 1172 (citing *Syphers* as persuasive and employing Fourth Amendment standard). Adopting the First Circuit's holding in *Syphers*, the *Brewer* court determined that evidence derived from a search, which was conducted under the authority of a validly issued state warrant, is considered lawful for federal prosecutorial purposes, as long as the warrant satisfies constitutional requirements and does not contravene the policies embedded in the Federal Rules of Criminal Procedure. *See id.* In determining that the warrants at issue were validly authorized under Missouri law, the court focused its Fourth Amendment analysis on the issue of whether executing the computer search after ten days amounted to undue delay that rendered the warrants stale. *See id.* at 1173.

50. *See id.* (reasoning staleness turns on whether information supporting warrants provided "'sufficiently close in time'" (quoting United States v. Palega, 556 F.3d 709, 715 (8th Cir. 2009))). In evaluating whether probable cause had dissipated, the court examined several factors, including the lapse in time since the warrant was issued, the nature of the property subject to search, and the kind of criminal activity at issue. *Id.* It concluded that the delay in execution had no effect on the determination of probable cause. *Id.* at 1173. Where the media at issue was electronically stored files that were in police custody, the nature of the evidence suggested that the media would continue to contain child pornography, and that probable cause would continue to exist even if the police did not review it for several months. *Id.*

51. *See, e.g.*, *In re* Search of 1046 N. 2d Ave., No. 2:05-MJ-28, 2006 WL 709036, at *6 (W.D. Mich.

warrant did so on the condition that the forensic search of the computer be conducted within thirty days of the physical execution of the warrant.[52] The police executed the first stage of the search, and seized two computers within five days of the warrant's issuance.[53] They then applied for and received a thirty-day extension to search the seized computers.[54] The examiner searched one of the computers within the new thirty-day period, but did not complete the search of the second computer until after that period had expired.[55] Although searches of both computers revealed child pornography, the *Brunette* court ruled that only those images derived from the first search were admissible because the government had "failed to adhere to the requirements of the search warrant and subsequent order" in its second search.[56]

These magistrate-issued, ex ante restrictions regarding the amount of time police have to conduct the computer-search stage of the warrant also occur at the state level.[57] In *People v. Strauss*, the police sought and obtained a warrant for the search and seizure of the defendant's apartment and five computers under the condition that the forensic examination of the computers be conducted within ninety days.[58] The forensic analyst completed his search within the specified ninety days, resulting in the successful prosecution of Rory Scott Tefkin.[59] His roommate, Nathaniel Strauss, was not charged in the indictment.[60] In 2006, two years after the police obtained the initial warrant, the police reopened an investigation into Strauss's alleged sexual conduct with minor children, and sought another warrant to search Strauss's five computers,

Mar. 17, 2006) (setting thirty days for government determination); United States v. Brunette, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (conditioning warrant on conducting forensic analysis within thirty days of physical search), *aff'd*, 256 F.3d 14 (1st Cir. 2001); People v. Strauss, 180 P.3d 1027, 1028 (Colo. 2008) (en banc) (limiting search to completion within ninety days of warrant execution); *see also* Kerr, *supra* note 36, at 1252-55 (highlighting ex ante restrictions on temporal scope of computer searches).

52. *See Brunette,* 76 F. Supp. 2d at 42.

53. *See id.* (analyzing facts at hand).

54. *See id.* The government originally obtained the search warrant on February 4, 1999, and executed the physical search on February 9, 1999, whereupon they seized the two computers. *Id.*

55. *See id.* The thirty-day extension allowed the government until April 8, 1999 to finish its examination of both computers, but the government search did not commence until April 10, 1999. *Id.*

56. *See Brunette*, F. Supp. 2d at 42. Noting that the government failed to offer a legitimate reason for the delayed second search, the court reasoned that failure to comply with the warrant requirements rendered the evidence gathered from the search of the second computer inadmissible. *Id.*

57. *See* People v. Strauss, 180 P.3d 1027, 1031 (Colo. 2008) (en banc) (holding self-imposed time limit for search does not preclude subsequent warrant for same item); *see also* Kerr, *supra* note 36, at 1253 (discussing *Strauss* and ex ante warrant restrictions at state level).

58. *See Strauss,* 180 P.3d at 1028. Pursuant to recommendations of his colleagues, the department's forensic analyst included the ninety-day time limit in the warrant as being sufficient to access all the hard drives. *Id.* He later testified at the suppression hearing, however, that the time limit should be eliminated because ninety days was an unrealistic deadline. *Id.*

59. *See id.* (providing facts of case).

60. *See id.* Although Strauss was not charged, the police retained possession of his computer because they were continuing to investigate allegations that he had been making child pornography. *Id.*

which the police department continued to have in its possession.[61] Arguing that the 2006 warrant violated an express condition of the 2004 warrant—insofar as under the 2004 warrant, the police department had only ninety days to conduct the forensic examination—Strauss filed a motion to suppress any evidence arising out of the subsequent forensic examination of his computer.[62] He maintained that the police department should not be able to obtain a new warrant to reexamine the same computers it already had in its possession for two years, which far surpassed the ninety-day deadline.[63] Although the court noted that warrants are time sensitive, and that excessive delay in execution may render the affidavit insufficient to substantiate probable cause, the court held that an ex ante, self-imposed time limit for executing the computer-search stage of a warrant does not preclude the police from obtaining a subsequent warrant to access the same item again.[64]

Regardless of whether courts have enforced temporal limitations by evaluating Fourth Amendment considerations after the fact, or by conditioning issuance of the warrant on time restrictions ex ante, the resulting opinions have lacked consistency regarding what constitutes a reasonable delay in execution.[65] Furthermore, the extent to which the magistrates issuing the ex ante restrictions are authorized to do so is unclear.[66] The result is that different defendants receive different outcomes, despite similar circumstances.[67]

B. Failure to Particularize How to Particularize

Although Rule 41(e) was specifically amended to address issues arising out of computer and other electronic media storage searches, the rule does not address what degree of specificity is required in a warrant to describe sought-after electronically stored information.[68] The Fourth Amendment requires that

61. *See id.*

62. *See Strauss*, 180 P.3d at 1029 (detailing procedural history).

63. *See* People v. Strauss, 180 P.3d 1027, 1029 (Colo. 2008) (en banc) (outlining Strauss's argument against computer evidence). The trial court granted Strauss's motion to suppress, finding the police were not authorized to "[re]open the file cabinet" after the time limit in the original warrant had expired, but later ruled that there was probable cause to substantiate both the 2004 and 2006 warrants. *Id.*

64. *See id.* at 1029-30 (deferring to past precedent, applying statutory requirements that warrant be executed without delay). The court rejected Strauss's argument that because the 2004 warrant had a ninety-day time limit, police could never obtain another warrant to access the same files. *Id.* Further, it reasoned that no constitutional or statutory provision bars police from obtaining a subsequent warrant to search evidence for which they have already obtained a warrant and which they already have in their possession. *See id.* at 1030. The court noted that self-imposed restrictions in an initial warrant have no further implications on a subsequent warrant, as long as probable cause has not gone stale. *See id.*

65. *See infra* Part II.B.

66. *See* Kerr, *supra* note 36, at 1251 (suggesting ex ante warrant restrictions introduce constitutional error).

67. *See infra* Part II.B (detailing inconsistencies resulting from lack of particularization).

68. *See* FED. R. CRIM. P. 41(e) advisory committee's notes to 2009 amendment (amended 2011) (commenting on reason for revision).

investigators execute narrowly tailored warrants limited by the scope of probable cause.[69] In order to comply with the Fourth Amendment, the magistrate issuing a warrant must determine that a government-initiated search is reasonable, and that a warrant states with adequate particularity for what the police are searching.[70] A warrant is sufficiently particularized if the investigating officers "can with reasonable effort ascertain and identify the place intended" for search, and nothing regarding what and where to search is left to the discretion of investigating officers.[71]

Traditional Fourth Amendment jurisprudence is designed to ensure that searches conducted pursuant to a warrant do not devolve into general searches in which a warrant sanctions broad authority for limitless search, irrespective of probable cause.[72] Significantly, the Supreme Court identified the scope of a lawful search as "defined by the object of the search and the places in which there is probable cause to believe that it may be found."[73] The Court placed particular emphasis on the specific physical contours of evidence sought and where the government could search for it.[74]

Applying traditional Fourth Amendment jurisprudence to search and seizure of digital evidence poses significant problems.[75] Computers and other digital

69. U.S. CONST. amend. IV; *see* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (holding warrant validity turns on information available to officers at time of warrant's issuance); *see also* Kerr, *supra* note 36, at 1241 (discussing particularity requirement); Robinton, *supra* note 2, at 317-18 (outlining history and framework of requirement); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 80 (1994) (providing warrant requirement applies anywhere one holds reasonable expectation of privacy).

70. *See Garrison*, 480 U.S. at 84 (requiring warrants to identify specific place of search and specific evidence for seizure); *see also* Robinton, *supra* note 2, at 318-19 (discussing particularity requirement). When determining whether probable cause exists to substantiate authorization of a warrant, a neutral magistrate must examine the facts and circumstances presented by the investigating officers in the warrant application. *See* Robinton, *supra* note 2, at 318. The magistrate may only issue a warrant after determining that there is a substantial basis to support the existence of probable cause to search the specified location, and to seize evidence listed in the application. *See id.* The warrant must describe with particularity both the location investigators intend to search, as well as items they intend to seize. *See id.* The particularity requirement is designed to protect an individual's privacy interest by ensuring each search is narrowly specified to the justifications presented in the application. *See id.* at 318-19.

71. *See* Steele v. United States, 267 U.S. 498, 503 (1925) (explaining what description sufficient to satisfy requirements).

72. *See Garrison*, 480 U.S. at 84 (providing manifest purpose of particularity requirement to prevent general searches); *see also* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 299-300 (2005) (suggesting physical-search rules do not adequately fit digital evidence contours).

73. United States v. Ross, 456 U.S. 798, 824 (1982) (noting probable cause does not exceed realistic appraisal of where evidence physically found).

74. *See id.* Although an individual's privacy interest "must yield to the authority of a search," probable cause to authorize such a search requires that the sort of item being sought is of size and form so that it may be discovered in the location that police seek to search. *See id.* at 823. The Court further qualified the scope of a lawful search, stating, "Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase." *Id.* at 824.

75. *See* 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.

storage media are capable of containing an immense amount of data, both of the innocuous and illegal variety.[76] Significantly, one can manipulate how each piece of data appears, such that a file-ending traditionally associated with an image may be manipulated to appear as a file-ending associated with a document.[77] Criminals are not inclined to label contraband as such, and a forensic examiner cannot determine whether a file-name or file-ending bears any resemblance to what a file contains without opening it.[78] As such, because traditional Fourth Amendment jurisprudence is contingent on particularity of the nature and location of items sought, it is problematic to apply.[79] Absent the ability to adequately identify where a particular file is located, every forensic examination has the potential to be overbroad and constitute a general search,

Comprehensive Drug Testing, Inc., 97 J. CRIM. L. & CRIMINOLOGY 1151, 1155 (2007) (discussing legal confusion concerning computer searches rendering Fourth Amendment application complex and undefined). Courts have tried various approaches to fit computers into existing Fourth Amendment jurisprudence, while others have abandoned the traditional framework entirely and applied special approaches. *See id. Compare* United States v. Hill, 322 F. Supp. 2d 1081, 1088-89 (C.D. Cal. 2004) (attempting to square computer searches with traditional Fourth Amendment jurisprudence), *aff'd*, 459 F.3d 966 (9th Cir. 2006), *superseded by statute*, 18 U.S.C. § 3509 (2006 & Supp. 2010), *with* United States v. Comprehensive Drug Testing, Inc. (*CDT II*), 579 F.3d 989, 998-99 (9th Cir. 2009) (abandoning traditional jurisprudence to account for special computer-related restrictions), *modified en banc*, 621 F.3d 1162 (9th Cir. 2010), *and* United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999) (providing computer searches require special approach).

76. *See* Corey J. Mantei, Note, *Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches*, 53 ARIZ. L. REV. 985, 987 (2011) (noting computer's immense storage capacity allows intermingling of criminal offenses and family photos); *see also* Winick, *supra* note 69, at 104 (discussing digital data's unique problem of mixing innocuous and criminal files). Because computers and other electronic-storage media are capable of containing larger quantities and varieties of information, an increased likelihood exists that private, personal information irrelevant to the search will also be seized and searched pursuant to an otherwise lawful investigation. *See* Winick, *supra* 69, at 105.

77. *See* United States v. Gray, 78 F. Supp. 2d 524, 527 n.5 (E.D. Va. 1999) (acknowledging computer files often misleadingly labeled especially if owner wants to conceal illegal material); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 544-45 (2005) (describing difficulty of searching for digital evidence which can be easily manipulated).

> It is easy to change the extension of a file. To hide a picture, a user might take a file saved with a '.jpg' extension and resave it with an extension common to a different kind of file, such as '.doc' or '.wpd.' A search for picture files based on the logical file extensions will no longer locate the file.

Kerr, *supra*, at 545.

78. *See* United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) (expounding tactics employed by criminals to conceal contraband); United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) ("[F]ew people keep documents of their criminal transactions in a folder marked 'drug records.'"). In the physical world, evidence specified in a warrant has certain characteristics, such as size and shape, that help police determine whether or not they can expect to uncover evidence in a particular location. *See* Robinton, *supra* note 2, at 323 (highlighting difference between physical and digital searches). The result is different in the digital context where "the location of evidence does not necessarily depend on the character of the evidence itself." *See id.* Because data is represented as a series of ones and zeros, the information's location and format is virtually impossible to predict, such that an investigator cannot rule out searching a particular part of the hard drive ex ante. *See id.*

79. *See* Robinton, *supra* note 2, at 323-24 (discussing inapposite nature of particularity requirement and digital evidence).

which is precisely what the Framers attempted to protect against.[80]

Courts have struggled to reconcile this issue with application of the plain view doctrine.[81] The plain view doctrine—an exception the Supreme Court carved out from Fourth Amendment protections—recognizes that there are limited, but legitimate police-enforcement interests in allowing the government to execute a warrant and seize evidence not particularly described in a warrant.[82] The plain view doctrine allows police officers to seize items not described with particularity, so long as three elements are satisfied: the officer must be lawfully in the location where the evidence is seized; the officer must have a "lawful right of access to the object itself"; and the incriminating nature of the object must be "immediately apparent."[83] Because it is virtually impossible for a forensic examiner to know what a file contains before opening it, the plain view doctrine seemingly allows one who is authorized under a warrant to claim that any incriminating evidence was in plain view, and thus admissible.[84]

80. *See* Saylor, *supra* note 12, at 2826 (suggesting failure to recognize problems inherent to computer warrants facilitates police discretion and general searches).

81. *See id.* at 2824-26 (discussing inapposite characteristics of computers and plain view doctrine); *see also* Kerr, *supra* note 72, at 280 (cautioning computer searches may allow "extraordinarily invasive government powers to go unregulated in some contexts"); Haynes, *supra* note 4, at 758 (addressing issues of applying traditional Fourth Amendment doctrines in modern context); Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J.L. & TECH. 120, 126-33 (2007) (providing courts' various unsuccessful attempts at reconciling computer searches and plain view doctrine).

82. *See* Horton v. California, 496 U.S. 128, 132 (1990) (stating plain view exception to general rule that warrantless seizures presumptively invalid); Coolidge v. New Hampshire, 403 U.S. 443, 467-69 (1971) (accounting for legitimate law-enforcement interest in seizing unspecified evidence discovered during lawful search); *see also* Trepel, *supra* note 81, at 126 (discussing plain view and container exceptions to Fourth Amendment protections).

83. *See Horton*, 496 U.S. at 136-37 (enumerating elements of plain view doctrine); *see also* Saylor, *supra* note 12, at 2819-22 (discussing elements and development of plain view doctrine). The *Horton* Court affirmed the holding in *Coolidge* that recognized the propriety of the plain view doctrine; nevertheless, the Court eliminated the requirement that police must inadvertently discover evidence, realizing it was problematic to apply and evaluate. *See Horton*, 496 U.S. at 130. The Court noted that "evenhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer." *Id.* at 138; *see* Saylor, *supra* note 12, at 2821 (discussing elimination of inadvertency requirement). Thus, the plain view doctrine stands for the proposition that if the officer is lawfully authorized to execute a search and finds an article of obviously incriminating evidence that is plainly visible, then detection and acquisition of that evidence does not count as an illegal search or a seizure under the Fourth Amendment. *See* Saylor, *supra* note 12, at 2819-20.

84. *See* Ziff, *supra* note 27, at 861-63 (analyzing existing application of plain view doctrine to computer searches). The ability to manipulate digital files and their extensions means that police are at a disadvantage if they are unable to search computers and other storage media broadly. *See id.* at 869 (explaining difficulties associated with Fourth Amendment protections as related to computers). However, the legitimate privacy interests that the Fourth Amendment was intended to safeguard are in jeopardy if police are able to search any file under the guise that incriminating information could reasonably be contained therein. *See* Kerr, *supra* note 72, at 304 (noting difference between traditional search and digital search). This tension has the ability to effectively broaden the scope of a warrant by allowing police to claim they were searching within the particularized terms of the warrant, yet still lawfully search a computer's hard drive. *See id.* at 304-05 (explaining objective judicial test for search). Additionally, courts will often defer to the investigator in

The circuits are split regarding how to apply the plain view doctrine, because the elements enumerated in *Horton* do not neatly translate to a digital environment, and Rule 41(e)(2)(B) fails to provide specific instructions for digital evidence in this context.[85] Even where police are searching for a specific file on a certain drive, the ability to disguise one file as another may necessitate a search of every file on the digital storage device.[86] There are effectively four approaches courts have taken to reconcile this issue.[87]

The Fourth Circuit applies the plain view doctrine to digital data no differently than physical evidence.[88] In *United States v. Williams*, the court analogized computer and other media-storage devices to a filing cabinet, stating that both were capable of containing large numbers of documents and amounts of information.[89] The court held that because it had successfully applied the plain view doctrine to searches of non-electronic files, the procedure and analysis should be no different for electronic files.[90] It reiterated that so long as the investigating officer's conduct satisfies the plain view elements established in *Horton*, a warrant authorizes a broad search and the ability to open and

determining what technology must be seized, because courts have explicitly acknowledged that the nature of a digital search makes it impossible to limit warrants with particularity. *See* Saylor, *supra* note 12, at 2826. As a result, law-enforcement officials applying for a warrant attempt to avoid drafting warrants in such a way as to restrict the scope of their search. *See id.* This result is in clear contravention of the Fourth Amendment's particularity requirement, and the Supreme Court's holding in *Marron v. United States* that an officer executing a search warrant should have no discretion. *See* 275 U.S. 192, 196 (1927) (limiting seizure to those items described by warrant); *see also* Saylor, *supra* note 12, at 2825 (explaining particularity requirement designed to limit intrusiveness of search).

85. *See Horton*, 496 U.S. at 136-37 (outlining elements of plain view doctrine); *see also* Moshirnia, *supra* note 12, at 612 (noting difficulty of applying plain view doctrine to digital setting).

86. *See* Moshirnia, *supra* note 12, at 612-13 (suggesting search for specific file may require search and seizure of every file); *see also* Saylor, *supra* note 12, at 2829 (proffering warrant execution methods inevitably more intrusive in digital context). Although courts have recognized that "brief perusal" of innocuous evidence is necessary to determine whether it falls within the scope of a warrant, this perusal is considerably more intrusive in the digital context because a digital search necessarily requires that every file be opened to determine whether its contents are incriminating—which is not the case in physical searches. *See* Saylor, *supra* note 12, at 2829-30 (reviewing problematic method followed by some courts).

87. *See supra* note 16 and accompanying text (suggesting circuit courts split regarding application of plain view doctrine to digital evidence). The Fourth Circuit has held that a traditional application of the plain view doctrine applies to digital evidence; the Seventh and Third Circuits have held that the plain view doctrine should progress incrementally in the digital context; the Tenth Circuit has held that analysis of the plain view doctrine should be fact driven, but officers cannot conduct a sweeping comprehensive search; and the Ninth Circuit has held that the traditional plain view doctrine should not apply to digital evidence. *See supra* note 16 and accompanying text.

88. *See* United States v. Williams, 592 F.3d 511, 521 (4th Cir. 2010) (upholding traditional application of plain view doctrine irrespective of electronic differences); *see also* Saylor, *supra* note 12, at 2831-32 (summarizing *Williams* and traditional application of plain view doctrine).

89. *Williams*, 592 F.3d at 523 (concluding quantity of information in computer does not distinguish it from traditional search). In *Williams*, police were investigating threatening messages sent to a Baptist elementary school. *Id.* at 514. The magistrate issued a warrant for "[a]ny and all computer systems and digital storage media, videotapes, videotape recorders, documents, photographs, and Instrumentalities indicat[ive] of the offense . . . ." *Id.* at 515.

90. *See id.* at 524.

cursorily view each file.[91] Additionally, the court rejected the defendant's argument that the plain view doctrine could not be applied to searches of computers or other electronic-storage devices when there is an indication that an officer planned to search for evidence by opening files that were not authorized by a warrant.[92]

The reasoning employed by the *Williams* court focused on differences between the defendant's privacy and possessory interests in the items being searched and seized.[93] The plain view doctrine applies to seizures but not searches; if an item is in plain view, its observation is not a violation of privacy, but its seizure would invade the owner's possessory interest, which is a protection implicated by the Fourth Amendment.[94] The *Williams* court reasoned that "*mere observation*" of evidence in plain view during execution of a lawful search does not implicate the Fourth Amendment, and therefore "does not need to be justified by any exception to the warrant requirement."[95] Furthermore, seizure of incriminating evidence is also justified, irrespective of the warrant requirement, because any ownership or possessory interest in it is "defeated by its illegality."[96]

Similar to the Fourth Circuit's approach, the Seventh and Third Circuits chose not to abandon the plain view doctrine in the digital context.[97] Rather than applying the doctrine exactly as they would in a physical search, however, the Seventh and Third Circuits chose not to afford broad authority to investigators, determining instead that the doctrine should progress

91. *See id* at 521-22. Because the warrant authorized a search of the defendant's computer and digital media for evidence relating to the threats, it impliedly authorized the investigating officers to open and view each file on the computer to determine whether or not the content fell within the scope of the warrant. *Id.* at 521-22.

92. *See id.* at 522. The defendant claimed that applying the plain view exception would "read . . . the warrant requirement out of the Fourth Amendment." *Id.* at 518.

93. *See Williams*, 592 F.3d at 521 ("The justification for the plain-view exception becomes evident when considering the difference between searches and seizures.").

94. *See* Horton v. California, 496 U.S. 128, 133-34 (1990) (discussing application of plain view doctrine to seizures but not searches); *cf.* Ziff, *supra* note 27, at 844 (discussing exception and application of plain view doctrine). Significantly, the courts have not determined that a search of a defendant's computer or digital data constitutes a seizure. *See* Kerr, *supra* note 77, at 557 (suggesting digital copying may not constitute seizure). Although the Supreme Court has characterized a seizure of property as "some meaningful interference with an individual's possessory interests in that property," indicating that searching a copy would constitute a seizure, subsequent case law has indicated that copying does not constitute a seizure. United States v. Jacobsen, 466 U.S. 109, 113 (1984) (providing seizure constitutes possessory interference with another's property); *see* Arizona v. Hicks, 480 U.S. 321, 324 (1987) (suggesting merely copying information does not seize anything); *see also* Kerr, *supra* note 77, at 557 (discussing implications of bit-stream copying as neither search nor seizure).

95. United States v. Williams, 592 F.3d 511, 521 (4th Cir. 2010).

96. *See id.*

97. *See* Saylor, *supra* note 12, at 2833-37 (characterizing Seventh and Third Circuits' approach as traditional but allowing for incremental progression of doctrine); Weir, *supra* note 3, at 98 (providing Seventh Circuit upheld plain view doctrine but did not fashion bright-line rule).

incrementally based on the facts and circumstances of each individual case.[98] In *United States v. Mann*, police executed a search warrant for evidence relating to a voyeurism charge on the defendant's computer, and ultimately identified file names associated with child pornography.[99] Reasoning that although a warrant is supposed to place limitations on a search, the Seventh Circuit decided that the ability for a criminal to hide incriminating evidence virtually anywhere indicates that the better approach to dealing with this issue is to "'allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication.'"[100]

Similarly, in *Stabile v. United States*, the Third Circuit held that the plain view doctrine applies to seizures of digital evidence, "but the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner."[101] In an attempt to reconcile the criminal's ability to manipulate files to conceal criminal activity—such that a broad and expansive search may be required to adequately identify criminal activity—with the proposition that "granting the Government a *carte blanche* to search *every* file on the hard drive impermissibly transforms a 'limited search into a general one,'" the court held that based on the facts of this case, the examiner properly discovered child pornography pursuant to the plain view exception elucidated in *Horton*.[102]

98. *See* United States v. Stabile, 633 F.3d 219, 240-41 (3d Cir. 2011) (rejecting approach that forswears plain view in digital context); United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010) (comparing case law to find common ground with digital application of plain view doctrine); *see also* Saylor, *supra* note 12, at 2833-37 (summarizing Third and Seventh Circuits' rejection of revisionist approach and adoption of incremental approach).

99. *Mann*, 592 F.3d at 780-82. The warrant was for "video tapes, CD's or other digital media, computers, and the contents of said computers, tapes, or other electronic media, to search for images of women in locker rooms or other private areas." *Id.* at 780-81.

100. *See id.* at 785 (quoting *CDT II*, 579 F.3d 989, 1013 (9th Cir. 2009), modified en banc, 621 F.3d 1162 (9th Cir. 2010)).

101. *See Stabile,* 633 F.3d at 241. In *Stabile*, Secret Service Special Agents were investigating allegations that Stabile had defaulted on his loans, and had tried to mask the default by passing more than $156,000 in counterfeit checks. *Id.* at 224. Upon executing the physical stage of the search warrant, the investigating agents found check-writing software and various other indicia of counterfeiting, but also subsequently seized the defendant's computers, as well as two DVDs that had titles indicating they were child pornography. *Id.* at 225. A forensic examiner applied for state warrants to search the computer and DVDs for "both financial crimes and the possession of child pornography." *Id.* at 226. During his search, the analyst found a "Kazvid" file, which references "Kazaa," a peer-to-peer file sharing system that is often used to trade child pornography. *Id.* at 226-27. Because Kazaa can be used for a variety of illegal activity, the examiner opened it and found twelve video files, all of which contained child pornography. *Id.* at 227. The examiner subsequently contacted the prosecutor on the case and applied for a warrant, basing probable cause on the names of the files in the Kazvid folder and not the content of the files. *Id.*

102. *See id.* at 237 (quoting Marron v. United States, 275 U.S. 192, 196 (1927)). Looking to other circuits for guidance, the *Stabile* Court ultimately did not invalidate the search for evidence of financial crimes, irrespective of the examiner's subjective belief that the Kazvid folder could contain child pornography, because evidence of financial crimes could reasonably be located within the file. *Id.* 238-41. Applying the elements enumerated in *Horton*, the court determined that the examiner did not violate the Fourth Amendment, that the incriminating nature of the evidence was immediately apparent, and that he had lawful right of access to the object of the search because the state search warrant authorized him to search the hard drive for evidence of

Central to both the Seventh and Third Circuit decisions was skepticism about requiring officers to obtain pre-approval from the authorizing magistrate to use electronic tools and digital searching devices to conduct searches "tailored to uncovering evidence that is responsive to a properly circumscribed warrant."[103]

The Tenth Circuit did not reject the plain view doctrine in the digital context, but instead held that because the officer in *United States v. Carey* knew he would uncover evidence beyond the scope of the warrant, and intentionally continued to search, the evidence was not in plain view.[104] In *Carey*, the investigating officer executed the digital stage of a warrant to search for evidence relating to sale and distribution of controlled substances, and in the process, discovered a file that alluded to, and in fact was, child pornography.[105] The officer abandoned his search for controlled-substance evidence and began looking exclusively for more evidence of child pornography.[106] Although the Supreme Court in *Horton* explicitly omitted any inadvertency requirement to the plain view doctrine, the *Carey* court noted that because the officer's subjective intent was to find something not authorized by the warrant, he violated the defendant's Fourth Amendment rights.[107]

financial crimes. *Id.* at 241-42.

103. *See Mann*, 592 F.3d at 785 (elucidating skepticism of Seventh Circuit); *see also Stabile*, 633 F.3d at 238 ("[I]t would be 'folly for a search . . .' because 'imposing such limits would unduly restrict legitimate search objectives.'" (quoting United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009))).

104. *See* 172 F.3d 1268, 1275-76 (10th Cir. 1999) (suggesting investigators use methods to avoid searching files not identified in warrant). The court rejected the concept that computer data was analogous to a file cabinet or closed container, because any such comparison oversimplifies the extent to which vast amounts of innocuous and incriminating information can be intermingled in the digital context. *Id.* at 1275. The court suggested that law enforcement should employ various methods to avoid searching for information not specified in the warrant, including performing a keyword search for relevant terms, observing file titles and formats, and reading portions of each file stored in the computer's memory. *Id.* at 1276. The Tenth Circuit's approach combines aspects of both the plain view doctrine and the closed container rule, which limits the scope of a search by permitting investigators to search only those containers that could reasonably hold items described in a warrant. *See id.*; *see also* United States v. Ross, 456 U.S. 798, 822-24 (1982) (indicating Fourth Amendment protects concealed contents of containers, but protection afforded varies in different settings); Trepel, *supra* 81, at 127 (summarizing Tenth Circuit's suggestion that courts acknowledge computer-specific issue of intermingled documents). Despite deciding that analogizing a computer to a container was inappropriate, the court determined that the investigator had, or should have had, probable cause to know that the files he was searching would not contain any evidence regarding the controlled substances investigation. *See Carey*, 172 F.3d at 1275.

105. *See Carey*, 172 F.3d at 1275. The warrant authorized the officer to search the computer files for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances." *Id.* at 1270. He began searching for key terms indicative of drug-related activity, and upon producing no such files, explored the computer's directory, where he found some files he was unable to view. *Id.* Upon downloading the files to a disk and opening one of them on another computer, the investigator discovered that it contained child pornography. *Id.*

106. *See id.* The officer proceeded to download nearly 250 more image files that contained child pornography before returning to his search for evidence of drug transactions. *Id.*

107. *See* Horton v. California, 496 U.S. 128, 138 (1990) (omitting inadvertency requirement from plain view analysis); *see also Carey*, 172 F.3d at 1276 (holding examiner exceeded search's scope by opening files with expectations of finding child pornography). In *Horton*, the Supreme Court indicated that requiring the plain view doctrine to turn on whether or not the officer discovered the evidence inadvertently is flawed,

In *Carey* and in subsequent cases, the Tenth Circuit made it clear that the nuances and complexities arising out of digital searches require a "special approach" to sort through electronic information, in order to protect against general warrants.[108] Following *Carey*, it clarified the special approach required to constitutionally limit computer searches of "intermingled documents," where the files being searched contain both relevant and irrelevant information.[109] In *United States v. Campos*, law enforcement obtained a warrant to search the defendant's computer for child pornography after receiving information that he had allegedly sent two images to an informant via email.[110] Although the court reiterated several limitations on the scope of computer searches, it determined that unlike in *Carey*, the search in the present case was not overly broad and had remained properly within the scope of the warrant, even though the investigating agent had uncovered more evidence than the two images

because objective standards of conduct are necessary for "evenhanded law enforcement." *Horton*, 496 U.S. at 138; *see supra* note 83. The Court went on to state that an officer's subjective suspicion that a file may contain incriminating evidence not within the scope of the warrant is immaterial if the officer lawfully executes a search for evidence within its scope. *See Horton*, 496 U.S. at 138. In this vein, the government in *Carey* argued that the situation presented to the investigating officer was similar to having lawful authorization via a warrant to search a file cabinet with multiple drawers. *See Carey*, 172 F.3d at 1274-75. The court rejected this argument, reasoning that because the detective "knew, or at least had probable cause to know, each drawer was properly labeled and its contents were clearly described in the label" his choice to search the child pornography files indicated that he was no longer searching for evidence authorized by the warrant. *Id.* at 1274. The subjective-intent test utilized by the Tenth Circuit required that every image discovered by the examiner, aside from the first, be suppressed. *Id.* at 1273. The court reasoned that although the officer discovered the first image inadvertently, other images were found only after he "temporarily abandoned" his search for evidence of drug trafficking, and instead began searching for evidence beyond the scope of the warrant. *Id.* The court drew heavily from Raphael Winick's argument that because of the vast quantities of information that computers contain, and the resulting intermingling of files, computer searches create a rapidly expanding threat that every warrant for a computer search has the propensity to authorize a general search. *See id.* at 1275-76; Winick, *supra* note 69, at 105. Winick's argument rejected the theory that comprehensive computer searches necessitate that the investigator peruse every file on the defendant's hard drive, and instead proffered that investigators should be limited to using key-word searches, or by looking only for the appropriate file type. *See* Winick, *supra* note 69, at 107-09 (suggesting investigator limit searches to keywords to find relevant files).

108. *See Carey*, 172 F.3d at 1275 n.7 ("[T]he storage capacity of computers requires a special approach . . . ."); United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) (providing examiner's "clear search methodology" preserved constitutionality of search); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000) (distinguishing facts of *Carey* but affirming special approach and particularization of computer search methodology); *see also* Trepel, *supra* 81, at 130 (summarizing Tenth Circuit's special approach to computer searches to avoid general warrants). *But see* United States v. Burgess, 576 F.3d 1078, 1092 (10th Cir. 2009) (providing "*Carey* holding was limited" and factually specific).

109. *See Campos*, 221 F.3d at 1148 (affirming but distinguishing *Carey*); Trepel, *supra* note 81, at 132 (suggesting file-sorting mechanism necessary to protect against general warrants).

110. *Campos*, 221 F.3d at 1145. The informant relayed to police that the defendant had sent him several pornographic images, including two images of child pornography, and thereafter provided the agents with a floppy disk containing the copied images. *Id.* Subsequently, the police obtained a warrant authorizing the agents to seize computer equipment, "which may be, or [is] used to visually depict child pornography, child erotica, information pertaining to the sexual activity with children or the distribution, possession, or receipt of child pornography, child erotica or information pertaining to an interest in child pornography or child erotica." *Id.* at 1147 (quoting language from search warrant).

referenced by the informant.[111] The court reasoned that the defendant had offered no evidence as to search methods employed by the investigating agent.[112] Subsequently, in *United States v. Walser*, the Tenth Circuit emphasized that the premise underlying *Carey* is that officers may not "conduct a sweeping, comprehensive search of a computer's hard drive" and claim anything discovered therein is in plain view.[113] The *Walser* court determined that the agent's search was reasonable because he used a clear and specific search methodology when examining the defendant's computer, ceased his search of the defendant's hard drive when he discovered child pornography not identified within the scope of the warrant, and then subsequently obtained a separate warrant to specifically search for child pornography.[114]

While most circuit courts have applied the plain view doctrine to discovery of digital evidence, the Ninth Circuit effectively rejected its applicability to electronic searches entirely.[115] In *United States v. Comprehensive Drug Testing, Inc.* (CDT), which arose out of a federal investigation into whether members of Major League Baseball were using performance-enhancing drugs, authorities secured a grand jury subpoena and warrant for the seizure of records and specimens of ten players whom the government had probable cause to search.[116] When authorities executed the warrant, they discovered a computer directory containing all computer files for the drug-testing program.[117] They subsequently used this information to apply for new warrants to seize the records for any player who had returned positive results, claiming they were

111. *See id.*

112. *See id.* at 1148. Expanding upon the need for a sufficiently particularized inquiry and search methodology discussed in *Carey*, the Tenth Circuit emphasized that when law-enforcement officials encounter files containing both relevant and irrelevant documents, police must employ some means of sorting them to search only ones specified in the warrant. *See id.* (citing Raphael Winick, *Searches and Seizures of Computers and Computer Data,* 8 HARV. J.L. & TECH. 75, 108 (1994)). If unable to properly determine which documents are relevant without searching them, police must cease the examination and apply for a warrant that specifies what sort of file they are seeking before resuming their search. *See id.* Because the defendant offered no evidence regarding the search methods employed by the agents, the *Campos* court determined that it need not consider whether police followed the approach outlined in *Carey*, and that evidence of child pornography need not be suppressed. *Id.* at 1148.

113. *Walser*, 275 F.3d at 986.

114. United States v. Walser, 275 F.3d 981, 986-87 (10th Cir. 2001).

115. *See* Moshirnia, *supra* note 12, at 613 (explaining Ninth Circuit's rationale for abandoning plain view doctrine in digital domain); Weir, *supra* note 3, at 99-104 (summarizing Ninth Circuit's rejection of plain view doctrine for digital searches); *infra* notes 116-22 and accompanying text (discussing Ninth Circuit's rejection of plain view doctrine in electronic searches).

116. *See* 513 F.3d 1085, 1089 (9th Cir. 2008), *rev'd en banc*, 579 F.3d 989 (9th Cir. 2009), *modified en banc*, 621 F.3d 1162 (9th Cir. 2010). In 2002, federal authorities began to investigate whether the Bay Area Lab Cooperative was distributing steroids to professional athletes. *Id.* The warrants issued to search records at both the Nevada and California facilities provided that "computer personnel" would evaluate and determine the most effective way to gather information, which included on-site data copying and equipment seizure, and would be authorized to search the data "authorized by the warrant," including that which had been copied on-site. *Id.* at 1092-93.

117. *See id.* at 1092.

authorized to do so pursuant to the plain view doctrine.[118]

The Players Association moved for the return of its seized equipment and data in both California and Nevada, and also moved in California to quash the subpoenas that resulted from the search, all of which were granted.[119] Upon review of the decision en banc, the Ninth Circuit did not dispute the government's argument that it was necessary to open every file in order to know its contents, but rejected the conclusion that every file was consequently admissible pursuant to the plain view doctrine.[120] The court reasoned that if the government must open every file to know its contents, it follows that "everything the government chooses to seize will, under this theory, automatically come into plain view."[121] Where the other circuits attempted to address this issue by adapting the plain view doctrine in the digital context, the Ninth Circuit held that both law enforcement's and the defendant's interests were better served if there were clear, prophylactic rules: "The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect."[122]

III. ANALYSIS

A. Time to Execute

Although Congress amended the Federal Rules of Criminal Procedure to resolve ambiguity that arises when applying traditional search-warrant rules to digital evidence, it ultimately did not go far enough.[123] Rule 41(e), as

118. *See id.* at 1094. Following execution of the warrant, the government issued several grand jury subpoenas to acquire more information. *Id.*

119. *See id.* The Major League Baseball Players Association sought the return of the seized data and equipment pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure. *Id.*; FED. R. CRIM. P. 41(g) (amended 2011) (providing one may move for return of seized property in unlawful search). Holding that the government's search procedures were improper, Judge Cooper of California determined that the government's actions failed to follow precedent, Ninth Circuit Judge Mahan of Nevada determined that the government had "callously disregarded . . . constitutional rights," and Ninth Circuit Judge Illston of California summarized the government's actions as harassment. *CDT*, 513 F.3d at 1094-95.

120. *CDT II*, 579 F.3d 989, 999 (9th Cir. 2009), *modified en banc*, 621 F.3d 1162 (9th Cir. 2010).

121. *See id.* at 998. The government argued that because it could not determine whether data was mislabeled, concealed, or compressed without examining the contents of every file, should it discover incriminating evidence unrelated to the evidence identified in the warrant, that evidence should be admissible according to the plain view doctrine. *Id.* at 997-98. Under this theory, the entire list of Major League Baseball players who had tested positive could be seized. *Id.* The court acknowledged the government's legitimate need to seize large quantities of data and sift through all of it in order to identify what falls within the scope of the warrant, but reasoned that applying the plain view doctrine to recovery of digital evidence "create[s] a powerful incentive for [the government] to seize more rather than less." *Id.* at 998.

122. *CDT III*, 621 F.3d 1162, 1177, 1180 (9th Cir. 2010) (en banc) (advocating prophylactic rules and setting forth guidelines for search and seizure of digital evidence).

123. *See* Kerr, *supra* note 36, at 1251-52 (recognizing timing requirement remains unclear despite 2009 amendment); Haynes, *supra* note 4, at 766 (indicating amendment did not extend far enough).

amended, differentiates search warrant procedure for digital evidence from physical evidence in several important ways: It specifically authorizes search and seizure of electronic-storage media or electronically stored information; it authorizes a "later review of the media or information consistent with the warrant"; and it notes that the timing requirements referenced in 41(e)(2)(A) and (f)(1)(A) pertain only to onsite copying of information and not later off-site forensic examination.[124] While this amendment clarifies that the Federal Rules do in fact recognize a distinction between digital and physical evidence, it provides insufficient clarity to substantively impact judicial determinations regarding whether a search warrant for digital evidence was executed in a reasonable time.[125]

As written, Rule 41(e) leaves the determination of timeliness for execution to individual magistrates.[126] When making such determinations, the Fourth Amendment, precedent, and the Federal Rules of Criminal Procedure typically guide decisions, but as outlined above, none are particularly helpful.[127] The case law following the 2009 Amendment illuminates the difficulties magistrates often face when determining timeliness of warrant execution.[128] Despite Congress's attempt to clarify how much later the off-site forensic examination could occur, different magistrates and reviewing judges continued to apply different standards in determining what constituted a reasonable amount of time.[129]

124. FED. R. CRIM. P. 41(e) & advisory committee's notes to 2009 amendments (amended 2011).

125. *See* Kerr, *supra* note 36, at 1251-52 (indicating 2009 amendment provides insufficient guidance); Haynes, *supra* note 4, at 766 (calling for further amendment to federal rules to provide greater guidance).

126. *See* Kerr, *supra* note 36, at 1252 (indicating magistrates have imposed their own timing limitation on search-warrant execution). Rule 41(e)(1) states, "The magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it." FED. R. CRIM. P. 41(e)(1) (amended 2011). Some magistrates mandate ex ante restrictions on warrants that specify an exact time period in which the digital stage of the warrant must be conducted. *See* Kerr, *supra* note 36, at 1252. The result is that search-warrant execution is regulated by two different sources of law: the ex post evaluations of Fourth Amendment standards of reasonableness, analyzed after a search has been conducted and the defendant has challenged the search's validity, and the ex ante restrictions that magistrates impose in an attempt to predict the reasonableness of how a warrant should be executed. *See id.* at 1281. The dual source-of-law regulation result is problematic because magistrates are making preemptive evaluations of reasonableness without actual facts on which to base that evaluation. *See id.* Consequently, law enforcement may be unnecessarily forced to comply with standards that are rendered moot by an ex post reasonableness review of the actual facts at issue. *See id.*

127. *See supra* Part II.B (detailing sources of guidance and noting lack of clarity); *see also* Kerr, *supra* note 36, at 1251 (pointing to Fourth Amendment and Federal Rules as authority governing timing for search warrant execution).

128. *See supra* notes 43-64 and accompanying text (examining case law decided after 2009 amendment). Some courts have interpreted the Fourth Amendment to govern the timing requirement. *See supra* notes 43-50 and accompanying text (discussing Fourth Amendment jurisprudence when determining temporal boundaries of digital search-warrant execution). In other cases, courts have upheld ex ante magistrate-issued restrictions on the timeliness required of digital search-warrant execution. *See supra* notes 51-64 and accompanying text (citing and discussing cases upholding magistrate-issued time requirements).

129. *See supra* notes 44-64 and accompanying text (highlighting different standards employed by courts). As previously indicated, certain magistrates avoided attempting to square the execution deadline with abstract

Certain legal scholars have suggested amendments to Rule 41(e)(2)(B) that would better address both the practical considerations and private rights implicated by search warrants for digital evidence.[130] Significantly, the central recommendation urges for a more definitive, bright-line requirement governing when a digital search warrant can be executed.[131] The policy behind these amendments is to impose more predictability, but the unique nature of digital evidence requires that each forensic investigation be tailored to the details and circumstances of each specific case.[132] Accordingly, although a bright-line rule will certainly impose predictability, such a rule must not be overly restrictive, and must be flexible enough to account for circumstantial variations.[133]

Taking these considerations into account, Congress should amend Rule 41(e)(2)(B) and set forth two specific rules to better govern timing of a digital-search process.[134] The first rule should charge a deciding magistrate with determining whether an electronic-media device is simply storage for digital evidence, or if it is an instrumentality of crime.[135] Based on that determination, the amount of time authorized for execution of a search should be decided according to a sliding scale, whereby a magistrate is allowed to grant the government anywhere from thirty days to twelve months to conduct the digital search.[136] Pursuant to this sliding scale, if a seized electronic-media device is

jurisprudential concepts, and instead imposed their own restrictions. *See supra* notes 51-64 and accompanying text (discussing attempts by magistrates to impose ex ante time restrictions).

130. *See* Kerr, *supra* note 1, at 129-32 (recommending changing Rule 41 to clarify when each step of warrant must be executed); Haynes, *supra* note 4, at 766 (providing "until the Committee amends the rules, the public's privacy interests will continue to suffer").

131. *See* Kerr, *supra* note 1, at 130 (suggesting implementing distinct rules to govern timing). "Rule 41 also should be amended to add clear guidance on when a computer must be searched and when it should be returned. Instead of leaving this to individual magistrate judges, a uniform standard should be used." *Id.* at 129-30.

132. *See id.* at 93-94 (highlighting need for flexibility regarding issues of warrant execution). In certain circumstances, the police will not be able to determine how long a particular search is going to take, how difficult the extraction will be, or what the lab's workload capability will be. *See id.* at 94.

133. *See id.* at 93-94 (discussing need for flexibility and predictability in amendment).

134. *See supra* Part II.A (exposing need for more sufficient guidance from federal rules).

135. *See* Kerr, *supra* note 1, at 130-31 (suggesting magistrates distinguish between evidence as storage or as instrumentalities); *see also* Brenner & Frederiksen, *supra* note 26, at 52 (opining distinction exists between digital storage devices and contraband, evidence, and criminal instrumentalities). Both *Syphers* and *Greene* indicate that irrespective of a warrant, an otherwise lawful search and seizure might be unconstitutional if law enforcement retains the target's property for too long. *See* United States v. Syphers, 296 F. Supp. 2d 50, 59 (D.N.H. 2003) (suggesting possible constitutionally imposed limits on seizure duration), *aff'd*, 426 F.3d 461 (1st Cir. 2005); United States v. Greene, 56 M.J. 817, 823 (N-M. Ct. Crim. App. 2002) (suggesting potential constitutional issues exist when extensive time elapses between seizure and return); *see also* Kerr, *supra* note 1, at 131 (proffering *Syphers* and *Greene* suggest constitutional issues arising from seizure duration). Alternatively, in crimes such as the possession and distribution of child pornography, or where the computer is being used to facilitate the crime, the computer serves as an instrument of the crime. *See* Kerr, *supra* note 1, at 131 (suggesting digital device's use as instrument of crime requires different rules).

136. *See* Kerr, *supra* note 1, at 131 (suggesting thirty days as reasonable minimum for executing digital warrants); *cf.* United States v. Triumph Capital Grp., 211 F.R.D. 31, 66 (D. Conn. 2002) (finding delay in execution exceeding one year reasonable given totality of circumstances). This sliding scale is designed to

more akin to a simple storage device, a magistrate should authorize an amount of time closer to thirty days; but if the media appears to be an instrumentality of crime, a magistrate should authorize time extending closer to twelve months.[137] If a device is merely a storage device, an individual's possessory rights to that device should be minimally infringed.[138] Depending on classification of the electronic media, a forensic examiner will need more time to determine whether it is a "fruit, instrumentality of crime, or contraband," and accordingly, whether an individual has any legal right to the property after the search.[139]

Congress should also extend Rule 41(e)(2)(B) to allow law enforcement to petition a magistrate for additional time to execute a digital search.[140] This rule is designed to account for the practical concerns and exigencies that arise when forensic examiners are performing searches in real time and not in an academic vacuum whereupon an uninterested magistrate can prospectively determine what is reasonable.[141] Under this rule, law-enforcement personnel are allowed to make a secondary showing to a magistrate that they need additional time to conduct the search.[142] In deciding whether to grant additional time, a magistrate should consider whether or not a device is for storage or is an instrumentality of crime, whether there are legitimate laboratory backlogs that have interfered with an expedited search, whether police and forensic examiners acted in good faith regarding the time it took to perform the search to date, and whether the particular search at issue is so complicated that it requires more time to perform.[143]

account for both the target's individual property rights, as well as practical law-enforcement concerns that arise when examiners perform these forensic searches—both of which were concerns central to the 2009 amendment. *See* FED. R. CRIM. P. 41(e) advisory committee's notes to 2009 amendments (amended 2011) (indicating unique digital evidence requires a substantial and unknowable amount of time to process); *see also* Kerr, *supra* note 1, at 132 (detailing goal of Rule 41 amendments).

137. *See* Kerr, *supra* note 1, at 131-32 (claiming rules must balance police exigencies and defendant's possessory interest). The individual whose possessory right is being interfered with should receive the device back more quickly. *See id.* at 131. If, by virtue of conducting the search, the forensic examiners determine that the storage device is in fact an instrumentality of the crime, then they need not return it, as the defendant has no legal right to possess contraband. *See id.*

138. *See id.* at 130. Because the examiner is able to conduct the analysis by using a byte-stream copy to the same effect as if he had the computer or storage device to work from, the individual is able to regain access to his property within a time period that is both reasonable and reflective of the time necessary for the examiner to access and copy the relevant evidence. *See id.*

139. *Id.* at 131-32 (suggesting different rule should apply for evidence used as instrumentality of crime).

140. *See id.* (asserting courts should allow examiners and police to apply for extensions).

141. *See supra* note 131 (noting unforeseen delays may result from complex digital searches or understaffed forensic labs).

142. *See* Kerr, *supra* note 1, at 130-31 (describing scenarios where examiners reasonably require additional time to execute warrant); *see also* Kerr, *supra* note 36, at 1252-55 (discussing difficulties of predicting ex ante reasonability).

143. *See* United States v. Mutschelknaus, 592 F.3d 826, 829 (8th Cir. 2010) (reconciling Rule 41 and magistrate-granted extension of execution); United States v. Syphers, 426 F.3d 461, 469 (1st Cir. 2005) (balancing reasonableness of delay against forensic lab backlog in determining constitutionality); *see also supra* note 135 (detailing reasonable time for searching storage devices versus instrumentality of crime or

B. Particularizing the Particularity Requirement

The 2009 advisory committee's note to Rule 41(e)(2)(B) indicates that the rule specifically declines to address the extent to which law enforcement must state with particularity what it intended to search for when applying for a search warrant for digital evidence.[144] This purposeful omission has been most problematic for courts that are confronted with challenges to the constitutionality of digital evidence discovered pursuant to the plain view doctrine.[145] Where both innocuous and incriminating information are often intermingled, file extensions can be manipulated to disguise a file's actual content, and there are virtually no means by which a forensic investigator can identify a file's content without opening it; even a sufficiently particularized warrant has potential to place every piece of digital evidence into plain view.[146] This directly contravenes the Framers' concerns with general warrants, which lead to general and constitutionally impermissible searches and seizures.[147]

The idea of balance is central to the Fourth Amendment; courts have historically balanced society's need for safety and security with an individual's interest in privacy and freedom from unwarranted intrusion by encouraging diligent and proactive law enforcement.[148] Absent guidance from Congress, circuit courts have split over the extent to which a warrant must be particularized such that the plain view doctrine is not implicated every time a forensic examiner executes a digital search warrant.[149] While none of the circuit-court approaches perfectly embody the requisite balance, some more

contraband); *supra* note 132 and accompanying text (discussing potential exigencies delaying digital search execution).

144. FED. R. CRIM. P. 41(e)(2)(B) advisory committee's notes to 2009 amendments (amended 2011). "The amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards concerning both the seizure and the search to ongoing case law development." *Id.*

145. *See supra* Part II.B (discussing continued ambiguity and inconsistent approaches to resolving particularity in digital contexts).

146. *See supra* notes 76-79 and accompanying text (examining unique problems with inability to differentiate innocuous and incriminating data on computers).

147. *See supra* note 80 and accompanying text (recalling how failure to reconcile intermingling issue facilitates general searches in contravention with Constitution).

148. *See* New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (stating reasonableness of search determined by balancing need for search against invasion that results); Oliver v. United States, 466 U.S. 170, 182-83 (1984) (evaluating government's intrusion on personal and societal values protected by Fourth Amendment); *see also* Moshirnia, *supra* note 12, at 628-30 (outlining balance between society's crime-prevention interest and individuals' privacy interest).

149. *See, e.g.*, *CDT III*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (declining to apply traditional plain view doctrine to digital evidence); United States v. Williams, 592 F.3d 511, 521 (4th Cir. 2010) (determining traditional plain view doctrine applies to digital evidence); United States v. Mann, 592 F.3d 779, 785-86 (7th Cir. 2010) (opining plain view doctrine should progress incrementally); United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) (holding plain view analysis fact driven, but officers cannot "conduct a sweeping, comprehensive search").

adequately address nuances arising out of this issue.[150]

The Fourth Circuit maintained that traditional rules governing particularity and the plain view doctrine adequately translate into the digital context, such that no special approach is required.[151] In not requiring more particularized search criteria, the Fourth Circuit fails to account for the possibility that even a particularized search warrant may implicitly authorize a general search.[152] Central to the Fourth Circuit's holding in *United States v. Williams* was the proposition that "mere observation" of evidence in plain view does not implicate the Fourth Amendment, and that seizure of such evidence poses no constitutional issue because its illegality severs an individual's possessory right.[153] Although the court's reasoning comports with a plain view analysis of physical evidence, it does not do the same in the digital context.[154] Holding that a privacy interest is not violated because the forensic examiner discovered evidence in plain view, the court did not acknowledge that, in the digital context, virtually every file has potential to be considered in plain view.[155] Keeping the constitutional goal of balance in mind, the Fourth Circuit's approach weighs heavily on the side of assisting law enforcement, without sufficiently protecting an individual's privacy interests.[156]

Taking the opposite approach, the Ninth Circuit determined that the plain view doctrine is completely inapplicable in the digital context, and therefore prescribed a number of prophylactic rules that prohibited the government from using it when executing digital searches.[157] Although the *CDT* court identified

150. *See infra* notes 151-74 (evaluating different circuit-court approaches).

151. *See Williams*, 592 F.3d at 521 (concluding plain view doctrine should apply as it does with physical evidence); *see also* Weir, *supra* note 3, at 106-07 (summarizing holding in *Williams*).

152. *See* Saylor, *supra* note 12, at 2849 (warning this approach permits discovery of unlimited incriminating information). If there are no means to discern the contents of a file without opening it, every file must be opened in order to ensure that the individual has not manipulated the file to disguise its incriminating content, and every search in effect becomes a general search. *See id.*; *see also* Weir, *supra* note 3, at 107 (discussing propensity for targeted searches to transform into general searches).

153. *See Williams*, 592 F.3d at 521; *see also supra* notes 93-94 and accompanying text (suggesting existing tension between defendant's privacy and possessory interests rests on search and seizure distinction).

154. *See* Weir, *supra* note 3, at 107 (criticizing how approach undermines fact that digital evidence not confined to physical space). In the physical context, a search is limited by where the item being searched for could reasonably be; but no such restriction exists with regard to digital evidence. *See id.* Accordingly, the discovery of any and all incriminating evidence may be characterized as a plain view observation, and is consequently fair game for prosecution. *See* Kerr, *supra* note 77, at 545 (describing process of locating specific document by looking through host of files).

155. *See* Saylor, *supra* note 12, at 2850 ("The traditionalist approach . . . essentially permits any incriminating information found when searching each individual file on a given digital database to be used as evidence."); Weir, *supra* note 3, at 107 (suggesting digital examinations run risk of transforming particularized inquiries into general searches).

156. *See* Saylor, *supra* note 12, at 2859 (noting approach permits conduction of dragnet searches, which Framers aimed to prevent).

157. *See CDT III*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc). The court reasoned that "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id.* at 1177. Although the Ninth

the aforementioned issues associated with applying the doctrine to digital evidence, it failed to offer a legitimate basis for eliminating the plain view doctrine from digital searches entirely.[158]

With respect to balancing competing interests, this approach protects an individual's right to privacy and protects against overly broad searches.[159] The Ninth Circuit's approach severely restricts law enforcement's ability to search for and utilize digital evidence.[160] By requiring law enforcement to waive use of the plain view doctrine, this approach not only impedes law enforcement's ability to perform its job and safeguard an important societal interest, but it also creates an additional burden of designing a search methodology that limits discovery of any evidence that lacks probable cause.[161] Such a constraint weighs heavily against law-enforcement efficacy and is not required by the Fourth Amendment.[162] By requiring police to stipulate search methodology before actually seizing evidence, this rule gives magistrate judges unprecedented authority to supervise search-warrant execution, and unnecessarily restricts the forensic-examination process.[163]

Compared to the Ninth and Fourth Circuits, the Seventh and Third Circuits took a far more balanced approach regarding how best to apply the plain view doctrine in the digital context by allowing for incremental progression of the doctrine based on the facts and circumstances of each case.[164] This

Circuit has since amended its decision so that the stated rules constitute guidance rather than circuit precedent, criminal defendants in other circuits have cited *CDT* to support the proposition that applying the plain view doctrine in a digital context is inapposite with safeguarding individual liberties from government intrusion. *See* Mantei, *supra* note 76, at 997 & n.91 (citing circuit cases where defendant relied on *CDT* to suggest computers deserve heightened protection).

158. *See* Mantei, *supra* note 76, at 999-1000 ("The Supreme Court has never interpreted the Fourth Amendment to require officers to specify the precise manner and methods by which they execute a search."); Weir, *supra* note 3, at 114 (summarizing critique that *CDT* creates a bright-line rule without support).

159. *See* Mantei, *supra* note 76, at 1000 (opining prophylactic approach seems efficient check on overbroad searches).

160. *See id.* (suggesting logistical issues associated with filtering relevant information disincentivizes digital forensic investigations). Requiring third parties or government agents to conduct forensic searches in order to expedite the process is expensive, difficult to implement, and impractical, because it requires parties less familiar with the case to conduct the search. *See id.* Such restrictions seriously impede law enforcement's ability to effectively investigate. *See id.*

161. *See id.* at 999 (summarizing prophylactic rules and effects).

162. *See id.* at 1000 (indicating Fourth Amendment does not require officers specify precise search methods).

163. *See* Mantei, *supra* note 76, at 1000. Forcing the police and examiners to identify their approach before actually examining the evidence at issue restricts the process and may impede the examiner from discovering relevant information, because he would be working outside of the methodology initially specified in the warrant. *See id.*

164. *See* United States v. Stabile, 633 F.3d 219, 240-41 (3d Cir. 2011) (rejecting approach that forswears plain view in digital context); United States v. Mann, 592 F.3d 779, 785-86 (7th Cir. 2010) (holding plain view doctrine should develop incrementally); *see also* Saylor, *supra* note 12, at 2833-37 (summarizing Third and Seventh Circuits' rejection of revisionist approach and adoption of incremental approach); *cf.* Weir, *supra* note 3, at 98 (noting Seventh Circuit upheld plain view doctrine but did not fashion bright-line rule).

circumstance-driven approach recognizes the practical reality that criminals often disguise criminal conduct—in the physical and digital world alike—and that restricting law enforcement searches to only those files that contain incriminating titles is a futile exercise.[165] By evaluating each case as it arises and allowing the doctrine to progress incrementally, this circumstance-driven approach does not overly restrict law enforcement from performing its job.[166] The problem with this is that "courts have made little progress in forming a workable doctrine."[167] Although utilizing an incremental approach avoids directly confronting the plain view issues with digital evidence, those issues will continue to become more complex as digital technology evolves.[168] Furthermore, absent more particularized guidance, individuals in different jurisdictions may receive varying verdicts on substantially the same facts.[169]

Finally, the Tenth Circuit has adopted a "special approach" to dealing with the plain view doctrine in the digital context.[170] This approach combines aspects of both the plain view doctrine and the closed container rule, which limits the scope of a search by permitting investigators to search only those containers that could reasonably hold items described in a warrant.[171] As such, the Tenth Circuit evaluates an examiner's methods of conducting a search in its

165. *See Stabile*, 633 F.3d at 240-41 (recognizing confines of doctrine vary by case); *Mann*, 592 F.3d at 787 (advocating incremental development of doctrine). The Seventh Circuit provided the ability to hide incriminating forensic evidence virtually anywhere in a digital container and this indicates that the more appropriate approach to dealing with this issue is to allow the doctrine to develop case-by-case. *See Mann*, 592 F.3d at 785. Similarly, the Third Circuit held that the plain view doctrine applies to seizures of digital evidence, "but the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner." *Stabile*, 633 F.3d at 240-41.

166. *See* Saylor, *supra* note 12, at 2849 (cautioning although approach doctrinally correct, it ignores actual disparity between officers' actions and Framers' intent).

167. *See id.* (suggesting courts still grapple with same issue faced with decade ago). "Allowing the doctrine to progress incrementally neither protects Fourth Amendment rights in the present nor guarantees a situation where Fourth Amendment rights are protected by a proper balance in the future." *Id.*

168. *See id.* "So long as the technology to limit searches sufficiently is not present, the inherent problems with digital searches may only grow with enhanced encryption techniques, data mining, and more dynamic methods of data storage." *Id.*

169. *Compare Mann*, 592 F.3d at 785 (holding invasive use of software acceptable practice), *and Stabile*, 633 F.3d at 240-41 (determining broad digital search reasonable under circumstances), *with CDT II*, 579 F.3d 989, 999 (9th Cir. 2009), *modified en banc*, 621 F.3d 1162 (9th Cir. 2010) (stating use of invasive software "may not be used without specific authorization in the warrant").

170. *See* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) (providing examiner's "clear search methodology" preserved constitutionality of search); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000) (distinguishing facts of *Carey* but affirming "special approach"); United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999) (adopting "special approach" to computer searches); *see also* Winick, *supra* note 69, at 104 (suggesting computers require special approach because vast storage capacity incentivizes overbroad searches); *supra* notes 104, 107 and accompanying text (elucidating Winick's influence on Tenth Circuit's special approach).

171. *See* United States v. Ross, 456 U.S. 798, 822-24 (1982) (indicating Fourth Amendment protects concealed contents of containers, but protection afforded varies in different settings); *see also* Trepel, *supra* note 81, at 127 (summarizing Tenth Circuit's suggestion that courts acknowledge computer-specific issue of intermingled documents).

analysis of whether execution of a warrant and subsequent plain view discovery were reasonable.[172] This method, while imperfect, recognizes that a special approach must be taken when applying the plain view doctrine to digital evidence.[173] Although restricting an examiner's ability to access every file may result in unrecovered evidence, not imposing any restrictions on the examiner's search methods and allowing him unlimited access to every data point on a storage device is tantamount to a warrant that allows the police to search one's entire house for anything and everything incriminating; such a general search is prohibited by the Fourth Amendment.[174]

Accordingly, the Federal Rules of Criminal Procedure should be amended in order to require courts to implement a modified version of the Tenth Circuit's approach.[175] The amendment would serve to provide a clear, explicit rule on how particularized a warrant must be in order to avoid allowing *every* warrant for digital evidence to implicate the plain view doctrine and devolve into a general search.[176] Although digital forensic technology is not presently capable of discerning whether a file contains incriminating evidence of the type described by a warrant without opening it, there are ways for an examiner to limit the scope of his search for items particularized in the warrant.[177]

172. *See Walser*, 275 F.3d at 986 (providing examiner's "clear search methodology" preserved constitutionality of search); *Carey*, 172 F.3d at 1276 (suggesting investigators use methods to avoid searching files not identified in warrant). In *Walser*, the investigating agent used a specific search methodology when examining the defendant's computer, and ceased his search when he discovered evidence not identified in the warrant, thereby avoiding a "sweeping, comprehensive search." *Walser*, 275 F.3d at 986-87.

173. *See* Ziff, *supra* note 27, at 852-58 (highlighting problems with Tenth Circuit's approach stemming from inadvertency requirement); *see also Carey*, 172 F.3d at 1276 (requiring inadvertent discovery of evidence). This approach "incorrectly relies on the subjective intent of the searching officer to determine the constitutional limits on the scope of a computer search," which is contrary to the principle outlined in *Horton v. California*. Ziff, *supra* note 27, at 853; *see also* Horton v. California, 496 U.S. 128, 138 (1990) (holding officer's subjective intent does not invalidate search and seizure). Additionally, the rigidity of stipulating a search methodology and applying for an additional warrant if the examiner discovers evidence not particularized poses an increased burden on examiners and law-enforcement officials that is not implicated by some of the other circuits' approaches. *See* Kerr, *supra* note 1, at 130 (discussing need for flexibility in digital search warrant execution); Mantei, *supra* note 76, at 1000 (highlighting logistical issues of requiring examiners to stipulate methodologies at outset of examination).

174. *See* Saylor, *supra* note 12, at 2829 (proffering warrant execution methods inevitably more intrusive in digital context); Winick, *supra* note 69, at 105 (cautioning execution of digital warrants may result in general searches); Moshirnia, *supra* note 12, at 613 (suggesting searches for specific files may require search and seizure of every file); *see also supra* note 76 and accompanying text (summarizing disconnect between warrants for physical and digital evidence).

175. *See supra* notes 170-74 (describing Tenth Circuit's special approach). While the Tenth Circuit's approach should be modified slightly, it recognizes that search warrants do not neatly translate from the world of physical evidence to digital evidence. *See* Kerr, *supra* note 72, at 304-06 (describing jeopardy to legitimate privacy interests if police able to search any file). Absent some sort of special method, police can conceivably search every inch of a suspect's computer, and reasonably claim they were searching within the terms of the warrant. *See id.* at 304-05.

176. *See supra* Part II.B (reviewing circuit split over most effective approach to particularizing warrants for digital evidence).

177. *See* Trepel, *supra* note 81, at 141 (indicating methods exist to narrow digital searches); Winick, *supra*

In applying for a warrant, the forensic examiner must attach an affidavit that he will use one of these types of search methods in executing the digital stage of a search.[178] If, in the course of searching for evidence particularized in a warrant via the method described in the application, an examiner opens a file and finds incriminating evidence not of the type sought by the warrant, he must cease the search and apply for a subsequent warrant to search for additional evidence of that nature.[179] Such a requirement not only provides greater protection for an individual whose property is being searched, but also shields government agents from misconduct claims, and secures the ability to admit evidence at trial.[180] Additionally, by requiring a forensic examiner to stipulate to search methods used, and by compelling the government to get a second warrant when necessary, the significance of inadvertency in the course of executing a warrant becomes much less material.[181] Such a requirement imposes a greater burden on the government, but it does not completely prohibit it from finding and using evidence for which it did not have probable cause at the outset.[182]

note 69, at 105-07 (suggesting certain forensic methodologies, like keyword searches, help limit scope of intrusion); Haynes, *supra* note 4, at 771 (providing methodologies for examiners to limit searches). Although the examiner need not be as limited in sticking to his methodology as Winick might suggest, there are "several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory." *See* United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999); *see also* Haynes, *supra* note 4, at 771 (indicating keyword and metadata searches helpful guides). Although the file extension may help guide the examiner, he should not be limited to searching only files with corresponding extensions. *See* Kerr, *supra* note 77, at 545 (describing futility of searching for incriminating digital evidence when file endings easily manipulated). In addition to file extensions, keyword searches can be particularly effective when the search is for specific documents with relatively predictable language. *See* Haynes, *supra* note 4, at 771. *But see* Brenner & Frederiksen, *supra* note 26, at 61 (suggesting usefulness of keywords searches often depends on sensitivity of context).

178. *See* Winick, *supra* note 69, at 108 (suggesting government specify anticipated methodology when applying for warrant); *cf.* Haynes, *supra* note 4, at 772 (maintaining proffered search methodologies reestablishes neutral role of magistrate). By requiring police and forensic examiners to provide a particularized search methodology, magistrates will be in an improved position to properly sort out unreasonable applications. *See* Haynes, *supra* note 4, at 772. Not every method need be the same, but requiring some kind of method helps ensure that a defendant in the Fourth Circuit will receive the same protections as that of a defendant in the Ninth Circuit. *Compare* United States v. Williams, 592 F.3d 511, 521 (4th Cir. 2010) (upholding traditional application of plain view doctrine irrespective of electronic differences), *with CDT*, 513 F.3d 1085, 1089, 1116 (9th Cir. 2008) (rejecting plain view doctrine in digital searches), *rev'd en banc*, 579 F.3d 989 (9th Cir. 2009), *modified en banc*, 621 F.3d 1162 (9th Cir. 2010).

179. *See Carey*, 172 F.3d at 1273 (requiring investigators obtain subsequent warrant upon discovering evidence not in original scope of search); *see also* Robinton, *supra* note 2, at 345 (reiterating holding in *Carey*).

180. *See* Robinton, *supra* note 2, at 345.

181. *See* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) (indicating examiner's "clear search methodology" ensured constitutionality of search). Requiring that the forensic examiner follow a specific methodology when executing the search suggests that subjective intent is less relevant in this analysis because the examiner is being held accountable to the methodology he submitted to the magistrate. *See id.*

182. *See* New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (reiterating reasonableness of search requires balancing need to search against extent of invasion); Oliver v. United States, 466 U.S. 170, 182-83 (1984) (evaluating whether "the government's intrusion infringes upon the personal and societal values protected by

IV. CONCLUSION

The advent of digital technology has created a unique set of problems for courts attempting to determine whether certain practices pertaining to search and seizure of digital forensic evidence are violative of the Fourth Amendment. In order to remedy some of these issues, Congress should further amend the Federal Rules of Criminal Procedure to close gaps that result from applying a 225-year-old doctrine to technology that continually evolves. Specifically, Congress should amend the federal rules to better govern timing of the digital-search process to provide more guidance to magistrates, defendants, and courts alike. Additionally, Congress should ensure that search warrants for digital evidence are particularized in such a way that forensic examiners can sufficiently search and discover evidence in plain view, but may not conduct general searches by virtue of the nuances associated with searching digital evidence.

Kaitlyn R. O'Leary

the Fourth Amendment"); United States v. Brignoni-Ponce, 422 U.S. 873, 878 (1975) ("As with other categories of police action subject to Fourth Amendment constraints, the reasonableness of such seizures depends on a balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers."); *see also* Moshirnia, *supra* note 12, at 628-30 (outlining balance between society's interest in preventing crime and individuals' privacy interest in being searched). By amending the rule as described above, the government is not completely barred from applying the plain view doctrine with digital evidence, as the Ninth Circuit would prescribe. *See CDT III*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc) (proffering government waive all reliance on plain view doctrine to safeguard individual privacy interests). Alternatively, there should be meaningful restrictions on what the government is allowed to recover in the course of executing a search warrant for digital evidence, so that issuance of a warrant does not authorize a general search. *See Williams*, 592 F.3d at 521 (4th Cir. 2010) (holding traditional plain view doctrine applicable).