Fordham Law Review

Volume 79 | Issue 6 Article 11

November 2011

Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches

James Saylor

COMPUTERS AS CASTLES: PREVENTING THE PLAIN VIEW DOCTRINE FROM BECOMING A VEHICLE FOR OVERBROAD DIGITAL SEARCHES

*James Saylor**

The plain view doctrine is based on the practical logic that an officer need not turn a blind eye to evidence that is immediately apparent as incriminating when he is lawfully present, where the object can be seen, and where he has a legal right to access that object. However, in the context of digital searches, this basic logic is stretched to a point that directly conflicts with the original purposes of the Fourth Amendment. The immense amount of data present on computers makes these searches much more intrusive. Officers employ search methods and techniques to access files that involve more investigation than the plain view doctrine ever intended. The problems presented by new technology to placing reasonable limits on the scope of otherwise valid Fourth Amendment searches have caused many courts to defer to traditional methods of analysis, rather than prompting courts to devise a new approach that could better reflect the realities of how police conduct these searches. Certain courts—which this Note designates "traditionalist"—find no reason to change what is a physical doctrine in the digital context, but rather allow it to progress incrementally.

This Note argues that courts have made no progress towards appropriately defining reasonableness in the context of digital searches, and that they should be imposing a heightened particularity standard for digital warrants, as well as additional prophylactic steps, as the U.S. Courts of Appeals for the Ninth and (to a lesser extent) Tenth Circuits have suggested. The traditionalist interpretation encouraged law enforcement authorities and training manuals to take advantage of this lax position, and plead general concerns common to all computer cases to justify broad search warrants. Moreover, the same general concerns that convince magistrates to draw such general warrants lead district court judges to defer to an investigator's discretion. To remain consistent with the original spirit of the Fourth Amendment, as a bar against unfettered police discretion and arbitrary governmental action, courts must adopt a new approach.

---

* J.D. Candidate, 2012, Fordham University School of Law. The author would like to thank his family and friends for their support during the production of this Note.

TABLE OF CONTENTS

INTRODUCTION

The police are executing a warrant on the home of a suspect accused of a minor crime. To prevent against indiscriminate rummaging by law enforcement, the warrant must lay out with particularity the area to be searched and the items to be seized. However, the warrant in this case is not for your average home. This particular suspect has all of his family's personal information, financial statements, medical information, and other effects strewn about the premises. Tax records are used as wallpaper, family photo albums form end tables in the living room, all personal correspondences are taped to the refrigerator, and so on. The intrusiveness of what would otherwise be a normal search, governed by normal Fourth Amendment principles, has been exacerbated by this wealth of information now available to an ambitious law enforcement officer. In executing this simple warrant, the officer justifies a dragnet search in which he is free to search and seize any portion of this wealth of data on the theory that it was all in "plain view."

This absurd example illustrates the difficulties courts face when they evaluate the appropriate limits of the "plain view" exception to the Fourth Amendment in the context of digital searches. When executing a warrant, the government may lawfully seize evidence of other crimes found in "plain view."[1] Like most exceptions to the warrant requirement, the plain view exception originally encapsulated practicality concerns, yet its scope has expanded as courts have become willing to find such exceptions present in changed circumstances.[2] The original justifications for the plain view doctrine are not present in digital searches,[3] and its wholesale adoption has

1. Horton v. California, 496 U.S. 128, 130 (1990).

2. *See* ROBERT M. BLOOM, SEARCHES, SEIZURES, AND WARRANTS: A REFERENCE GUIDE TO THE UNITED STATES CONSTITUTION 102 (2003).

3. *See* Arizona v. Hicks, 480 U.S. 321, 326–27 (1987) (describing the initial justification for the plain view exception in digital searches).

led to an impermissible dilution of the probable cause and particularity standard,[4] as well as the exclusionary rule.[5] Courts too easily analogize digital and physical searches, failing to see the plain view doctrine as essentially grounded in practicality concerns only present in physical environments—carefully delineated situations where it would be nonsensical to force an officer to ignore evidence that he stumbled upon in the course of an otherwise lawful physical search.[6]

Previously unforeseen circumstances introduced by new technology have made it more difficult to employ this reasoning, which was established in the context of physical searches. Hard drives have replaced filing cabinets, comprehensive financial and medical records are stored in massive databases, and some of our most personal information, including pictures of loved ones and personal correspondences, are stored in the almost endless space that exists on a modern personal computer.[7] The existence of all this information is compounded by the rise of data transmission over the Internet and the availability of access to thousands of employee files on businesses' shared databases.[8] Electronic storage contains much more information, both in terms of quantity and variety, which makes it a tempting target in a search for incriminating information.[9] Computers do not only hold information voluntarily stored. Unbeknownst to many users, they also "record and store a remarkable amount of information about what users write, see, hear, and do."[10] Because of this, analogizing electronically stored information to physical objects for the purposes of establishing constitutional limits, is an "oversimplif[ication that] ignores the realities of massive modern computer storage."[11]

The methods law enforcement employ to search computers afford them broad discretion to sift through these massive databases.[12] Warrants for

4. The particularity requirement is contained in the text of the Fourth Amendment and requires that "no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

5. The exclusionary rule states that evidence seized in violation of the Fourth Amendment cannot be admitted at trial. This rule was first applied to the federal government in the case of *Weeks v. United States*, 232 U.S. 383, 398 (1914). It was not until *Mapp v. Ohio*, 367 U.S. 643 (1961) that the Court applied it to the states via the due process clause of the Fourteenth Amendment. *Id.* at 660. For a more thorough discussion of the exclusionary rule, see 1 WAYNE R. LAFAVE, SEARCHES AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1 (4th ed. 2004).

6. *See infra* Part I.D.

7. United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) (stating that for the average user, computers are "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more" (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005))).

8. *See* Commonwealth v. Ellis, Nos. 97-192, 1999 WL 823741, at *34 (Mass. Sup. Ct. Aug. 18, 1999).

9. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 104–05 (1994).

10. Kerr, *supra* note 7, at 532.

11. Winick, *supra* note 9, at 110.

12. See *infra* Part II.

electronic files grant a license to investigating officers to conduct a general search while relying on the plain view exception to cover any evidence of crimes not contained in the warrant. The U.S. Supreme Court has held that the plain view exception "may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."[13] The Framers drafted the Fourth Amendment in the wake of the British colonial government's abuse of general warrants and writs of assistance that afforded investigating officers unfettered discretion in searching persons and places.[14] The spirit of their rejection of these tactics has continued to inform courts when evaluating Fourth Amendment issues.[15] With this history in mind, what should courts find to be "plain view" in the context of computer searches?

Circuit courts have disagreed on the appropriate standard. The United States Courts of Appeals for the Third, Fourth, and Seventh Circuits—a group this Note labels "traditionalist"—have not changed the doctrine in these new circumstances, and prefer to allow it to progress incrementally.[16] In contrast, the U.S. Court of Appeals for the Ninth Circuit,[17] and to a lesser degree the U.S. Court of Appeals for the Tenth Circuit[18]—a group this Note designates "restrictive"—have suggested a high particularity standard in warrants for digital evidence, including search protocols and other

13. Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).

14. *See infra* Part I.A–B.

15. *See infra* Part I.C–D.

16. *See* United States v. Stabile, 633 F.3d 219, 233–34 (3d Cir. 2011) (accepting the traditionalist approach and expressly rejecting measures suggested by the U.S. Court of Appeals for the Ninth Circuit); United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010) (finding it prudent to allow the doctrine to progress incrementally); United States v. Williams, 592 F.3d 511, 524 (4th Cir. 2010) (finding "no reason to depart" from the traditional test). While the Seventh Circuit arguably employed a unique semi-subjective test, its adherence to an incremental approach and rejection of ex ante restrictions make it deserving of a traditionalist classification. *But see* Orin Kerr, *Plain View for Computer Searches Generates Two Circuit Splits in Two Days:* United States v. Williams *and* United States v. Mann, THE VOLOKH CONSPIRACY (Jan. 21, 2010, 11:41 PM), http://volokh.com/2010/01/21/plain-view-for-computer-searches-generates-two-circuit-splits-in-two-days-united-states-v-williams-and-united-states-v-mann/.

17. United States v. Comprehensive Drug Testing, Inc. (*CDT III*), 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, J., concurring) (offering a safe harbor of prophylactic rules for officers to follow in searches of electronic storage devices). The Ninth Circuit, in an en banc opinion, originally made these prophylactic rules binding before revising their opinion after protest by the federal government. *See* United States v. Comprehensive Drug Testing, Inc. (*CDT II*), 579 F.3d 989, 1006 (9th Cir. 2009). For a discussion of the political pressure exerted by the executive after this opinion, see, for example, Thomas R. Eddlem, *Fourth Amendment Under Seige (Again)*, NEW AMERICAN (Nov. 28, 2009, 1:00 PM), http://www.thenewamerican.com/index.php/usnews/constitution/2420-Fourth-amendment-under-seige-again; David Kravets, *Obama Wants Computer Privacy Ruling Overturned*, WIRED (Nov. 25, 2009, 10:27 AM), http://www.wired.com/threatlevel/2009/11/obama-wants-computer-privacy-ruling-overturned/.

18. The U.S. Court of Appeals for the Tenth Circuit's original decision breaking from the traditionalist approach advocated a subjective standard. United States v. Carey, 172 F.3d 1268, 1273–75 (10th Cir. 1999). Later circuit decisions interpreted the *Carey* opinion as raising the particularity standard for warrants for digital evidence, where files are so intermingled as to necessitate limitations. *See* United States v. Burgess, 576 F.3d 1078, 1092–93 (10th Cir. 2009); United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).

prophylactic measures designed to prevent general dragnet searches from occurring.

Part I of this Note examines the history behind the drafting of the Fourth Amendment, the creation of the plain view doctrine, and how the underlying principles and justifications are strained in the context of computer searches and seizures. Part II examines the procedures used in executing digital searches and the inherent problems associated with particularly describing places to be searched on computers. Part III explores the conflict among the circuits introduced above. Part IV proposes that the current approaches employed by the circuits are inadequate, and that prophylactic rules similar to those suggested by the Ninth Circuit[19] are necessary to protect the fundamental right afforded by the Fourth Amendment to freedom from arbitrary governmental intrusion and unfettered police discretion.

I. THE ORIGINAL PRINCIPLES OF THE FOURTH AMENDMENT, THE COURT'S DEPARTURE FROM THESE PRINCIPLES, AND THE DEVELOPMENT OF THE PLAIN VIEW EXCEPTION

The formative history and principles of the Fourth Amendment animates judicial analysis when determining how the Fourth Amendment and the plain view exception should apply to new situations.[20] Courts have consistently looked to this formative history when analyzing Fourth Amendment issues,[21] but the use of a reasonableness balancing approach in many cases has weakened the historical approach.[22] This section discusses the Fourth Amendment's history to emphasize the spirit that should compel the formulation of a new regime to govern digital searches where traditional methods lead to the kind of search that the Fourth Amendment was drafted to prevent. Part I.A examines the resistance to overbroad and unreasonable searches and seizures that began in Great Britain. Part I.B explains the resistance to such practices in the colonies. Part I.C discusses the interpretation of the Amendment from the drafting to the present day and the development of the balancing approach. Lastly, Part I.D discusses the development of the plain view exception.

---

19. *CDT III*, 621 F.3d at 1178.

20. *See generally* M. Blane Michael, *Reading from the Fourth Amendment: Guidance from the Mischief That Gave it Birth*, 85 N.Y.U. L. REV. 905 (2010).

21. *See, e.g.*, Arizona v. Gant, 129 S. Ct. 1710, 1720 (2009); United States v. Chadwick, 433 U.S. 1, 7–9 (1977); Chimel v. California, 395 U.S. 752, 760–61 (1969); Katz v. United States, 389 U.S. 347, 356–57 (1967); Frank v. Maryland, 359 U.S. 360, 363–71 (1959); United States v. Di Rie, 332 U.S. 581, 595 (1948); Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting); Boyd v. United States, 116 U.S. 616, 622–23 (1886).

22. The balancing approach employed by many courts attempts to measure "the degree [of intrusion] upon an individual's privacy" against "the degree to which it is needed for the promotion of legitimate governmental interests." Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

A. The English Foundations of the Fourth Amendment and the Rejection of Overbroad Police Discretion

The notion of a natural right to privacy and freedom against arbitrary governmental intrusion predated the strong reactions against general warrants and writs of assistance that immediately precipitated the American Revolution. The Magna Carta, the great charter of English liberties, was widely interpreted as conveying rights against arbitrary governmental intrusion.[23] This interpretation has converted the Magna Carta into a "talismanic symbol of freedom" and helped instill this notion of privacy from as early as the 16th century.[24] Yet, prior to the American Revolution, the courts and English Parliament threatened this natural right through the issuance of general warrants and writs of assistance. General warrants only required a bare assertion that an officer suspected a violation of law, without any particularized information.[25] Writs of assistance did not require any justification or judicial supervision and were valid until the death of the sovereign.[26] These broad warrants gave officers a license to search wherever they wanted for whatever items they wished.

The practices employed by the English crown were completely incongruous to the popular rhetoric of the time. Some of the most influential legal theorists decried the specter of general warrants, including Sir Edward Coke, Sir Matthew Hale, William Hawkins, and Sir William Blackstone.[27] The old adage that a "man's house is his castle" had become commonplace from its origins in the early sixteenth century, and its influence converged with this movement.[28] William Pitt's famous quote to Parliament in 1763 read: "The poorest man may in his cottage, bid defiance to all forces of the Crown."[29]

The popular rhetoric among the academic community reflected that of the judiciary as well. One famous series of cases involved general warrants issued for the arrest of anyone involved with John Wilkes's controversial criticism of the Crown in the 45th volume of his journal, popularly known as "No. 45."[30] Wilkes filed suits of trespass against the officials involved and emerged as a popular idol for the cause against general warrants and arbitrary government action.[31] Judges in the "Wilkes cases" found such general warrants to be contrary to fundamental liberties,[32] and articulated

23. *See* LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 151 (1999).

24. *See id.* at 151–52; *see also* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 671–73 & n.341 (1999).

25. LEVY, *supra* note 23, at 154–55.

26. *Id.* at 155–57.

27. *See* THE COMPLETE BILL OF RIGHTS: THE DRAFTS, DEBATES, SOURCES, AND ORIGINS 242–44 (Neil H. Cogan ed., 1997); LEVY *supra* note 23, at 152; Davies, *supra* note 24, at 578–79.

28. BLOOM, *supra* note 2, at 5; LEVY, *supra* note 23, at 151–52; Davies, *supra* note 24, at 642 & n.259; Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 197–98 & n.3 (1993).

29. BLOOM, *supra* note 2, at 5.

30. LEVY, *supra* note 23, at 159.

31. *Id.* at 159–61; Davies, *supra* note 24, at 562–68.

32. Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (K.B.) 491.

that "it is not fit, that the . . . judging of the information should be left to the discretion of the officer. The magistrate ought to judge; and should give certain directions to the officer."[33] In the later case of *Entick v. Carrington*,[34] Lord Camden held that the power to issue warrants was limited by law and could not issue on executive discretion.[35] This judicial reaction is a result of the breach of common law tradition generally requiring a particularized warrant.[36]

B. Colonial Reactions to General Warrants and the Exercise of Unfettered Discretion by the Government

The American colonies inherited this controversy in 1696, when King William III extended authority to issue writs of assistance to the colonies, predictably resulting in widespread abuses.[37] When first extended to the colonies, the writs of assistance were a localized controversy,[38] yet they were issued against considerable resistance.[39]

These abuses led colonists to challenge the use of general warrants in the courts. In 1761, six months after the death of King George II, the chief customs official in Boston petitioned for new writs of assistance in the Massachusetts Superior Court.[40] James Otis, a Boston lawyer, appeared before the court on behalf of the people of Boston to oppose the writs. Otis argued that the writ was an instrument of "slavery," an exercise of "arbitrary power" and that the only legal writ was a "special warrant directed to specific officers."[41] The court did not side with Otis, and issued the general writ.[42] However, this case further spurred the cause of independence and the feelings of discontent within the colonies.[43] John Adams, prior to the signing of the Declaration of Independence, said that Otis's "[a]rgument concerning Writs of Assistance . . . [was] the [c]ommencement of the Controversy between Great Britain and America."[44]

In the period leading up to the Declaration of Independence, specific warrants increasingly gained favor among the legal community in

33. Money v. Leach, (1765) 97 Eng. Rep. 1075 (K.B.) 1088.
34. (1765) 95 Eng. Rep. 807 (K.B.).
35. *Id.* at 817–18.
36. *See* BLOOM *supra* note 2, at 7; Davies, *supra* note 24, at 655–57; Daniel M. Harris, *The Return to Common Sense: A Response to "The Incredible Shrinking Fourth Amendment"*, 22 AM. CRIM. L. REV. 25, 27–28 (1984).
37. BLOOM, *supra* note 2, at 5; Davies, *supra* note 24, at 659 n.306.
38. Prior to 1767, only Massachusetts and New Hampshire had expressly extended the jurisdiction of the English court authorized to issue writs of assistance to their highest courts. LEVY, *supra* note 23, at 157. In 1767, the Townshend Acts extended the jurisdiction of the Court of Exchequer to the highest courts of all the colonies. *Id.* at 163–64.
39. BLOOM, *supra* note 2, at 5.
40. *Id.* at 6. There is no case report for this decision, which is known colloquially as the "Writs of Assistance Case" or "Paxton's Case." Davies, *supra* note 24, at 561 n.20.
41. LEVY, *supra* note 23, at 158.
42. BLOOM, *supra* note 2, at 6.
43. Davies, *supra* note 24, at 561–63 & n.2l; Maclin, *supra* note 28, at 221–22 & n.80.
44. LEVY, *supra* note 23, at 157–58 (omission in original).

America.[45] After the passing of the Townshend Acts—extending the authority to issue general writs to the highest courts in all the colonies in 1767—some courts resisted the issuance of general warrants by imposing conditions that frustrated their execution.[46] Other judges expressly refused to issue the writs as "unconstitutional" or because they felt "without legal authority" to do so.[47]

After the signature of the Declaration of Independence, states began enacting their own constitutions, each with its own "bill of rights" that invariably contained some rejection of general warrants or a broader condemnation of the arbitrary governmental practices that existed under colonial rule.[48] The Massachusetts constitution was the first to frame the right as freedom from "unreasonable searches, and seizures."[49] At the time, the term "unreasonable" meant "violative of fundamental legal principles."[50] This interpretation of "unreasonable" by the Framers, and the multiple drafts of the Amendment, illustrate that they would find any searches conducted under warrants that did not conform to common law requirements—constrained by specific restrictions, issued upon probable cause, and determined by an independent magistrate—to be unacceptable.[51]

After hostilities with England ended, few states still employed general searches, and specific warrants became commonplace.[52] In the debates over the drafting of the Constitution, leaders proposed a bill of rights that omitted several of the rights considered fundamental today, but included a search and seizure provision.[53] James Madison introduced the initial language for the Fourth Amendment to the 1st Congress on June 8, 1789,[54] and the final text came to read:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[55]

---

45. *Id.* at 158–59; *see also* Maclin, *supra* note 28, at 224–26.

46. LEVY, *supra* note 23, at 164; Maclin, *supra* note 28, at 224–26. For example, the New York courts at first issued writs of assistance, but deviated from the language of Parliament, and after five years of being held up, found them to not be "warranted by law." LEVY, *supra* note 23, at 164. Virginia issued writs of assistance in 1769 but attached to them specific instructions found obnoxious by the customs office. *Id.* at 165.

47. LEVY, *supra* note 23, at 165.

48. For example, Virginia's Declaration of Rights reads "general warrants . . . are grievous and oppressive, and ought not be granted." VA. CONST. OF 1776, § 10. Pennsylvania followed suit, framing the protection as a "right" of the "people." PA. CONST. OF 1776, art. X; *see also* THE COMPLETE BILL OF RIGHTS, *supra* note 27 at 232–37.

49. MA. CONST. OF 1780, art. XIV.

50. BLOOM, *supra* note 2, at 8; *see* Davies, *supra* note 24, at 576–83.

51. *See* THE COMPLETE BILL OF RIGHTS, *supra* note 27, at 223; Davies, *supra* note 24, at 684–86; Harris, *supra* note 36 at 28–29.

52. LEVY, *supra* note 23, at 172–73; *see* BRUCE A. NEWMAN, AGAINST THAT "POWERFUL ENGINE OF DESPOTISM" 7 (2007).

53. LEVY, *supra* note 23, at 173; *see also* Davies, *supra* note 24, at 693.

54. BLOOM, *supra* note 2, at 9.

55. U.S. CONST. amend. IV.

While the details of how the final wording in the Bill of Rights came to be agreed upon are not available, it is clear from writings at the time that the principle was to secure the "great and valuable privileges" of freedom from unreasonable searches granted "with[out] due caution."[56] The Fourth Amendment was an essential protection to the Framers, one that assured the freedom supported by a centuries-long tradition of common law and legal theorists.[57]

C. The Fourth Amendment from the Drafting to the Present

The adoption of the Fourth Amendment enormously influenced the early government's behavior. In guaranteeing the freedom from unreasonable search and seizure, the Framers declared a broad principle that discretionary police power could not be trusted.[58] It was no longer acceptable for an officer to simply swear that he was acting in good faith and with probable cause to obtain a warrant with insufficient judicial scrutiny.[59]

The federal courts did not have an early opportunity to significantly interpret the Amendment, but early state cases indicate that the prevention of the exercise of broad power of the police was how the Fourth Amendment was understood to protect the people.[60] The first time the Supreme Court considered the issue was in *Boyd v. United States*,[61] almost 100 years after the Amendment's drafting. A unanimous Court found that forcing citizens to produce invoices to prove that certain items were not smuggled involved an exercise of "arbitrary power" by the government.[62] In the Court's first opportunity to interpret the Fourth Amendment, it held that the right of the people should be "liberally construed" and a "close and literal construction . . . leads to a gradual depreciation of the right."[63] The Court continued to apply these principles three decades later in *Weeks v. United States*,[64] where the Court again emphasized its concerns about the discretionary power of law enforcement, endorsing the use of particularized warrants to combat this discretion.[65] Later, in *Johnson v. United States*,[66] the Court held that a warrant's scope should be left to the judgment of a magistrate, rather than to the discretion of an "officer engaged in the often competitive enterprise of ferreting out crime."[67]

---

56. THE COMPLETE BILL OF RIGHTS, *supra* note 27, at 238–39 (quoting THE ANTI-FEDERALIST No. 1 (Centinel), No. 4 (The Federal Farmer)).

57. *See* Harris, *supra* note 36, at 29.

58. Maclin, *supra* note 28, at 229. This discretion was widely believed to be unlawful at common law. Davies, *supra* note 24, at 578–79.

59. LEVY, *supra* note 23, at 178.

60. Davies, *supra*, note 24, at 613.

61. 116 U.S. 616 (1886).

62. *Id.* at 630.

63. *Id.* at 635.

64. 232 U.S. 383 (1914).

65. *Id.* at 389–92; *see also* BLOOM, *supra* note 2, at 13.

66. 333 U.S. 10 (1948).

67. *Id.* at 14. In *United States v. Lefkowitz*, 285 U.S. 452 (1932), the Court echoed this sentiment by stating that the "informed and deliberate determinations of magistrates . . . are to be preferred over the hurried action of officers." *Id.* at 464.

In *Olmstead v. United States*,[68] the dissent found that the original principles underlying the Fourth Amendment should influence how it applies to new technologies by reiterating that the Amendment should not be limited to its words or "papers and effects," and that it was meant to protect a general right to be free from unreasonable government interference.[69] The majority to which the *Olmstead* dissent was responding was later overturned in *Katz v. United States*,[70] where the Court again emphasized the unpalatable discretion afforded to police when the judiciary is absent from the warrant application process.[71]

Despite these early cases that consistently followed the underlying principles and motivations of the Fourth Amendment, the murky historical record of the drafting—and the ambiguous text itself—allowed the Court to interpret the Fourth Amendment to achieve whatever results were convenient.[72] The debate on how the Framers intended the two clauses to be read led to the reasonableness clause[73] being read distinctly from the warrant clause,[74] resulting in a much broader balancing test.[75] The reasonableness approach allows for greater discretion for police officers and greater intrusions by the government. The Framers had a much stronger view against this, but the "doctrinal evolution has been away from a sense of the individual's right to be secure from government intrusions and toward an ever-enlarging notion of government authority to intrude."[76] As one commentator has stated: "The constitutional lodestar for understanding the Fourth Amendment is not an ad hoc reasonableness standard; rather, the central meaning of the Fourth Amendment is distrust of police power and discretion."[77] Some argue that this interpretation of reasonableness under the balancing approach advocated by the Court is contradictory to that of the Framers.[78]

D. The Development of the Plain View Doctrine

The plain view doctrine generally stands for the proposition that when an officer is lawfully present where he can see incriminating evidence and has

68. 277 U.S. 438 (1928).
69. *Id.* at 487–88 (Butler, J., dissenting).
70. 389 U.S. 347 (1967).
71. *See id.* at 358–59.
72. BLOOM, *supra* note 2, at 3; Davies, *supra* note 24, at 557–60; *see* Maclin, *supra* note 28, at 237 n.140.
73. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV.
74. "[A]nd no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*
75. BLOOM, *supra* note 2, at 14. Again, the Framers' understanding of "unreasonable" came from Sir Edward Coke and was a synonym for illegality—not the flexible standard that the Court chose to adopt. Davies, *supra* note 24, at 576–83.
76. Davies, *supra* note 24, at 749.
77. Maclin, *supra* note 28, at 201.
78. *See supra* notes 50–51 and accompanying text.

a legal right of access to that evidence, his detection of such evidence does not constitute a search or seizure for Fourth Amendment purposes.[79] A warrant is not necessary for the plain view doctrine to apply.[80] Yet, one of the most prototypical examples of its application is where the police have a warrant to search specific premises for objects related to a certain crime, and happen upon incriminating evidence relating to crimes or suspects not contained in the warrant.[81] As this historical discussion will show, the Court has continuously stated that the plain view exception was not to be used to permit searches that resembled general warrants.

The principle that officers, in the course of an otherwise constitutional search, can seize evidence not particularly described in a warrant has not always been clear. In *Marron v. United States*[82]—a case preceding the creation of the plain view exception—officers executed a search warrant for intoxicating liquors and articles of their manufacture.[83] The officers also seized ledgers and bills of illegal sales of liquor.[84] While the Court ruled that these items were lawfully seized incident to the arrest,[85] it also held that the particularity requirement made "general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer."[86] This created an inherent inconsistency: If no discretion is to be left to the officer, why is it acceptable that this discretion is exercised when an arrest is made on the premises?[87]

Lower courts struggled to rectify this inconsistency in *Marron*.[88] Because of this confusion, courts throughout the twentieth century declined to follow *Marron*, and the Supreme Court implicitly recognized the propriety of the plain view doctrine. The literal interpretation of the particularity discussion in *Marron* led courts to find that items could not be seized unless they were specified in the warrant, even if they were immediately incriminating.[89] Many courts distinguished *Marron* on the grounds that the ledgers seized were not obviously contraband,[90] or to disregard the doctrine when the items seized were stolen property.[91] Later, the Supreme Court noted that practicality justified the inclusion of evidence found in plain view because "it would be entirely without reason to say that

79. 1 LAFAVE, *supra* note 5, § 2.2.

80. *See* Coolidge v. New Hampshire, 403 U.S. 443, 465–66 (1971). The *Coolidge* Court described cases where evidence is seized in plain sight while in "hot pursuit" of a subject, incident to a lawful arrest, and when under the authority of a search warrant. *Id.*

81. *Id.* at 465.

82. 275 U.S. 192 (1927).

83. *Id.* at 193–94.

84. *Id.* at 194.

85. *Id.* at 198–99.

86. *Id.* at 196.

87. 1 LAFAVE, *supra* note 5, §4.11(b).

88. *Id.*

89. *See* United States v. Coots, 196 F. Supp. 775, 779 (E.D. Tenn. 1961).

90. *See, e.g.*, United States v. Eisner, 297 F.2d 595, 597–98 (6th Cir. 1962); Joyner v. City of Lakeland, 90 So. 2d 118, 122 (Fla. 1956).

91. *See* Johnson v. United States, 293 F.2d 539, 540 (D.C. Cir. 1961).

[an officer] must return [evidence] because it was not one of the things it was his business to look for."[92]

In its more recent discussions, the Court has limited the breadth of the plain view exception by continuing to evoke the animating principles behind the drafting of the Fourth Amendment.[93] In *Coolidge v. New Hampshire*,[94] any doubt as to the propriety of the plain view exception was put to rest. The Court in *Coolidge* affirmatively recognized the long history of cases recognizing the exception, while still reminding the government that "the 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."[95] The Court noted that allowing seizure in plain view did not contradict the purposes of the Fourth Amendment because plain view does not occur until a valid search is in progress, and that the seizure of objects in plain view does not convert that search into a general or exploratory one.[96] The *Coolidge* Court proceeded to outline the elements necessary to find an object seized in plain view, including a requirement that the police must have "inadvertently" come upon the items seized.[97]

The "inadvertency requirement" became problematic because the Court did not explain what degree of expectation was required to make discovery inadvertent.[98] Thus, the Court eliminated this requirement in *Horton v. California*[99] by holding it to be a characteristic of most legitimate plain view seizures but not a "necessary condition."[100] The Court held 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."[101] It rested its assumption that inadvertence was not necessary to protect police from conducting a general search on the fact that this interest is already protected by "scrupulous adherence" to the particularity requirement.[102] The *Horton* Court outlined the three-prong test used today to evaluate whether evidence collected other than that contained in a search warrant was properly seized under the plain view exception: the law enforcement officer must be lawfully present where the evidence may be plainly viewed, he or she must have lawful

92. Abel v. United States, 362 U.S. 217, 238 (1960).

93. Stanley v. Georgia, 394 U.S. 557, 572 (1969) ("To condone what happened here is to invite a government official to use a seemingly precise and legal warrant only as a ticket to get into a man's home, and, once inside, to launch forth upon unconfined searches and indiscriminate seizures as if armed with all the unbridled and illegal power of a general warrant."); United States v. Lefkowitz, 285 U.S. 452, 465 (1932) ("Here, the searches were exploratory and general and made solely to find evidence of respondents' guilt of the alleged conspiracy or some other crime."); Steele v. United States, 267 U.S. 498, 501 (1925) (discussing in depth the particularity requirement).

94. 403 U.S. 443 (1971).

95. *Id.* at 466.

96. *Id.* at 467.

97. *Id.* at 468–71.

98. 1 LAFAVE, *supra* note 5, § 4.11(e).

99. 496 U.S. 128 (1990).

100. *Id.* at 130.

101. *Id.* at 138.

102. *Id.* at 139–40.

access to the item itself and, the incriminating character of the evidence seized must be "immediately apparent."[103]

Indeed, the Court's discussion of the particularity requirement emphasized that the warrant clause's "manifest purpose" was to prevent general searches.[104] As outlined in the following sections, the execution of warrants for the search of computers and the lower courts' loose application conflict with this professed purpose.

II. SEARCH AND SEIZURE OF COMPUTERS

The procedures involved in obtaining and executing warrants for digital evidence implicate the Framers' concern over unfettered police discretion discussed in Part I.[105] The nature of digital evidence and the investigatory techniques employed by the government compel the creation of a new scheme to protect these original concerns. Several scholars of criminal justice contend that the Fourth Amendment has and will continue to be applied flexibly in digital evidence cases because of the uncertainty that exists in adapting to this new medium[106]—a flexibility that the Court has warned against in the past.[107] Part II.A first explains the inherent differences between the search of physical environments and the search of computers and other digital storage devices. Part II.B outlines how these warrants are obtained and executed to illustrate the difficulties faced in attempting to preserve the Constitutional mandates of the Framers and the Supreme Court.

A. The Inapposite Characteristics of Physical and Digital Searches

The plain view doctrine, as defined in physical environments, takes on a different context in digital searches. Officers do not interact with digital data in the same way, and with the same basic intuitions, as the dwellings considered by the Framers in drafting the Fourth Amendment. The plain view exception is based on sight, a notion that is very simple to apply in the context of a physical environment, but which becomes more difficult with computers.[108] Plain view could be defined as just what is open on the screen, whatever an officer decides to open, or some balance in between.[109] Moreover, physical environments can only contain a limited amount of objects and data, which limits the intrusiveness of allowing everything in

103. *Id.* at 136–37.
104. *Id.* at 139–40 n.10.
105. *See supra* Part I.
106. *See* ROBERT MOORE, SEARCH AND SEIZURE OF DIGITAL EVIDENCE 80 (2005); Arthur J. Carter, IV & Audrey Perry, *Computer Crimes*, 41 AM. CRIM. L. REV. 313, 350–55 (2004) (discussing flexible approaches applied in the courts); Sheri A. Dillon et. al., *Computer Crimes*, 35 AM. CRIM. L. REV. 503, 526–28 (1998) (same). Courts have explicitly noted that flexibility is necessary. *See* United States v. Sawyer, 799 F.2d 1494, 1508 (11th Cir. 1986).
107. *See supra* note 63 and accompanying text.
108. Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 93–94 (2002).
109. *Id.* at 94.

plain view to be seized. Computers hold a wealth of information, with capacity doubling every two years as technology advances.[110]

The constraints of physical environments make it unreasonable to search for a stolen car inside a house, or for any number of items that cannot physically be in the area searched.[111] This consideration is not present with the fungibility of computer files. Numerous judges have made the observation that any "clever suspect" does not store illicit materials with a file name indicating their contents.[112] This has led courts to find that investigators cannot be restricted in their search of all computer files.[113]

The duration of the search also differs significantly. In physical environments, the search ceases when the officers leave. By contrast, the massive information on computers often necessitates that they be copied and searched off-site by an investigator.[114] Law enforcement will copy the entire hard drive, and investigators are normally free to take whatever time is needed within reason to sort through this information.[115]

Compared to a physical environment, there is much less control over what data is stored on a computer. In the context of a physical environment, items can be positively destroyed. In contrast, files marked for deletion on computers can still be recovered by investigators; as long as a user does not reuse a particular "cluster" of data, the file marked for deletion will remain undisturbed, and "slack space" on a hard drive can even save this information after reuse.[116] Temporary files created by programs like Microsoft Word and the automatic data retention of Internet browsers also add to this confusion.[117] And as computers become integrated in businesses and people's daily lives, it is more often necessary in normal criminal investigations that do not involve cyber-crimes to search a suspect's computer.[118] The question of what rules should govern these searches is of utmost importance.

As a starting point, what constitutes a "search" or "seizure" of computer data that would trigger the protections of the Fourth Amendment is not

110. Kerr, *supra* note 7, at 542.

111. Kerr, *supra* note 7, at 543; *accord* Arizona v. Hicks, 480 U.S. 321, 324–25 (1987); United States v. Ross, 456 U.S. 798, 824 (1982).

112. Michael, *supra* note 20, at 926; *see also* United States v. Hill 459 F.3d 966, 978 (9th Cir. 2006); United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990); United States v. Gray, 78 F. Supp. 2d 524, 527 (E.D. Va. 1999).

113. *See* United States v. Williams, 592 F.3d 511, 521–22 (4th Cir. 2010) (approving an officer's search of every file on a computer because of the potential for concealment of evidence); United States v. Miranda, 325 F. App'x 858, 860 (11th Cir. 2009) (same); United States v. Hill, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004) (rejecting defendant's proposed search methodologies as restrictive because they provide too much potential for this type of camouflage); *see also infra* Part II.B.3.

114. MOORE, *supra* note 106, at 79.

115. *See infra* notes 165–67 and accompanying text.

116. Kerr, *supra* note 7, at 542; *see also* OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 62 (2009) [hereinafter OLE MANUAL], *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

117. Kerr, *supra* note 7, at 542–43.

118. *Id.* at 532.

completely settled. In physical environments, entering a home or other physical environment and moving or seizing objects therein constitutes a search. However, in the context of computers, police officers do not "enter" the computer nor do they view the raw data upon it; they merely sift through the billions of individual strings of data and either open the data onto a display to view at the scene, copy the data, or take no action.[119] This Note follows the Supreme Court and other prior decisions interpreting Rule 41 of the Federal Rules of Criminal Procedure.[120] These cases hold that copying constitutes a seizure, regardless of whether the officers actually ever search this copied data.[121]

B. How Law Enforcement Investigators Execute Warrants for the Search of Computers

This section discusses the execution of search warrants for digital data to illustrate how loose restrictions complicate Fourth Amendment issues in later review. Part II.B.1 explains the process for applying for a computer warrant and the requirements imposed by the Fourth Amendment. Part II.B.2 addresses the imposition of ex ante limitations on such warrants. Part II.B.3 generally discusses the common process used to search computers. Lastly, Part II.B.4 outlines the practical effects of these methods.

1. The Application and Contours of the Computer Warrant

Several sources provide guidance for law enforcement on what needs to be described in a warrant and the appropriate process for obtaining magistrate approval. Rule 41 of the Federal Rules of Criminal Procedure generally addresses warrant requirements, but has not provided specific instructions for digital evidence until recent amendments to the rule. Rule 41(e)(2)(B), as amended, explicitly states that warrants may issue for the seizure of electronic evidence for later review.[122] At least one commentator has suggested that this and other provisions alone authorize the broad scope of digital searches and seizures.[123] Courts have not yet analyzed recent amendments to Rule 41 that include information about digital searches, however they support some of the practices already in place in collecting digital data.

The Office of Legal Education of the Executive Office for U.S. Attorneys has published a manual on the search and seizure of computer evidence to

119. *Id.* at 540. Professor Kerr suggests that only the viewing of computer data constitutes a search that would trigger Fourth Amendment concerns. *Id.* at 556–57.

120. Rule 41 of the Federal Rules of Criminal Procedure, "Search and Seizure," governs the procedures surrounding the execution of search warrants generally. FED. R. CRIM. P. 41.

121. *See, e.g.*, United States v. N.Y. Tel. Co., 434 U.S. 159, 168–70 (1977) (explaining what constitutes a search in the context of pen registers); Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 706–07 (2010).

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

123. *See generally* 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 (2010).

guide prosecutors and law enforcement.[124] The requirements for an affidavit and application for a warrant to search a computer are substantially the same as for a physical environment. First, the investigator must state that he has probable cause to believe that the computer "*contains* or *is* contraband, evidence of a crime, fruits of crime, or an instrumentality of a crime."[125] The government endorses the comparison to a container to explain that no special facts are necessary to establish probable cause to authorize the search of a computer found on premises contained in a warrant, so long as investigators "reasonably believe the warrant describes records that might be stored on that computer."[126] However, *United States v. Payton*,[127] a case from the Ninth Circuit, seemed to tighten this standard from "could" produce evidence to "would" produce evidence[128]—causing the government to endorse the need for specific authorization to search computers.[129] Probable cause can be based on, inter alia, an IP address, online account information, and off-line conduct.[130]

Second, a warrant must also "particularly describ[e] the place to be searched, and . . . things to be seized."[131] Again, the Supreme Court has required sufficient particularity such that no discretion is left to the officer executing the warrant.[132] This requirement is meant to prevent the issuance of general warrants and to delimit a narrow search that will keep the level of intrusion to a minimum.[133] Except in the case where the actual computer is used as the instrumentality of a crime,[134] the warrant must describe the content of the relevant files rather than the storage device itself.[135] Courts have found this requirement to be more stringent in the context of computers because of the "huge array" of information that they are capable of containing.[136]

---

124. OLE MANUAL, *supra* note 116.

125. *Id.* at 63 (citing FED. R. CRIM. P. 41(c)).

126. *Id.* at 64 (internal citations omitted). Several courts have drawn this comparison. *See* United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007); United States v. Runyan, 275 F.3d 449, 462–63 (5th Cir. 2001); United States v. Barth, 26 F. Supp. 2d 929, 936–37 (W.D. Tex. 1998); United States v. Blas, No. 90-Cr-162, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990) (stating that a computer, pager, or similar devices must be treated as a "closed container"); *but see* United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999).

127. 573 F.3d 859 (9th Cir. 2009).

128. *See* Susan A. Rados, Note, United States v. Payton*: Redefining the Reasonableness Standard for Computer Searches and Seizures*, 40 GOLDEN GATE U. L. REV. 297, 299 (2010).

129. OLE MANUAL, *supra* note 116, at 65.

130. *Id.* at 65–68.

131. U.S. CONST. amend. IV.

132. *See* Marron v. United States, 275 U.S. 192, 196 (1927).

133. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

134. This situation arises primarily in the execution of search warrants for child pornography. OLE MANUAL, *supra* note 116, at 71 (collecting cases).

135. *Id.* at 72; *see also* United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (stating that description of particular files must be included in warrant).

136. United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009).

Failure to narrow the scope of a warrant through limiting terms can turn such a non-specific warrant into an unconstitutional general warrant.[137] Still, many courts have failed to recognize the problems inherent in computer warrants that allow investigators to essentially go through every file and seize evidence of other crimes under the plain view doctrine.[138] Courts have explicitly acknowledged that they are unable to limit warrants with particularity because of the nature of technology,[139] and they will defer to the discretion of the investigator to determine what property must be seized to obtain the evidence.[140] Seizing upon this leeway granted by many courts, the government has explicitly instructed law enforcement to "[a]void drafting warrants in a way that would unnecessarily restrict the scope of the search."[141]

Where particularity cannot be achieved because of the commingling of evidence and innocent files, some new restrictions may be necessary to prevent investigators from exercising unfettered discretion.[142] However, courts too often find that sufficient limiting terms are not possible, and choose to disregard search methodologies contained in the warrant because they are impractical.[143] Rather than allowing these situations to develop, the techniques for issuing these warrants should change to react to this problem.

2. Ex Ante Limitations on Computer Search Warrants

The Government has stated that limitations on search methodologies can seriously impair an investigator's ability to uncover evidence in computer searches.[144] Scholars similarly have stated that such ex ante regulations are "constitutionally unauthorized and unwise."[145] Digital searches "can be as

137. *See, e.g.*, *id.*; United States v. Ford, 184 F.3d 566, 576 (6th Cir. 1999) (collecting cases).

138. *See, e.g.*, United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010); United States v. Upham, 168 F.3d 532, 535–37 (1st Cir. 1999) (holding a warrant to not be overbroad where the officers had to search everything to ensure they found the relevant evidence); United States v. Gray, 78 F. Supp. 2d 524, 528–31 (E.D. Va. 1999) (same).

139. *See, e.g.*, *Williams*, 592 F.3d at 522; United States v. Reyes, 798 F.2d 380, 383 (10th Cir. 1986).

140. *See* United States v. Stabile, 633 F.3d 219, 239–40 (3d Cir. 2011); United States v. Mann, 592 F.3d 779, 782–83, 786 (7th Cir. 2010); United States v. Hill, 19 F.3d 984, 987–89 (5th Cir. 1994); Hessel v. O'Hearn, 977 F.2d 299, 301–02 (7th Cir. 1992).

141. NAT'L INST. OF JUSTICE, U.S. DEPT. OF JUSTICE, DIGITAL EVIDENCE IN THE COURTROOM: A GUIDE FOR LAW ENFORCEMENT AND PROSECUTORS 10 (2007) [hereinafter DIGITAL EVIDENCE IN THE COURTROOM].

142. *Cf.* United States v. London, 66 F.3d 1227, 1238 (1st Cir. 1995) (holding that in a situation where innocent documents were intermingled with the evidence sought it would be "difficult for the magistrate judge to be more limiting" in phrasing the warrant). See *infra* Part IV for a discussion of proposed limitations.

143. OLE MANUAL, *supra* note 116, at 76–79 (collecting cases).

144. *Id.* at 79–83 (discussing at length the basis for refusing to limit a search through search methodologies).

145. Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1244–45 (2010).

much an art as a science" that require on-the-spot judgment.[146] The government has further opined that magistrate-issued restrictions on warrants are unnecessary because ex post judicial review is sufficient to protect constitutional rights.[147] Still, in recent history, magistrate judges have begun to impose restrictions on the method and means by which a digital search may be conducted to cope with the specific problems discussed above.[148] These methods have found support among scholars who believe that Fourth Amendment rights continue to be diminished as old practices are grafted into new circumstances.[149]

Professor Orin Kerr has put forth the argument that the use of ex ante regulations by magistrate judges is constitutionally impermissible.[150] In making this assertion, he points to several Supreme Court cases that seem to prescribe a narrow role for magistrate judges. In *Lo-Ji Sales, Inc. v. New York*,[151] the Supreme Court found it impermissible for a magistrate judge to accompany officers on a search to make real time judgments of whether certain films constituted obscenity.[152] In *Dalia v. United States*,[153] the Court found that the absence of instructions on how exactly a wiretap would be installed did not render the warrant void for lack of particularity.[154] And in *United States v. Grubbs*,[155] the Court found that an anticipatory warrant[156] did not require ex ante restrictions for the triggering condition to be considered valid.[157] Kerr maintains that these cases are evidence that only certain minimum facts are necessary to satisfy the particularity requirement.[158] Kerr suggests that Justice Scalia's admonition in *Grubbs* that there is no general particularity requirement besides the place to be searched and things to be seized forecloses the use of ex ante limitations in computer searches.[159]

Putting aside the issue of their permissibility, ex ante limitations could take several forms, such as: (1) "conditions limiting the seizure of computer hardware during the physical search," (2) "conditions limiting the permitted timeframe of the electronic search," (3) "conditions on how the electronic search stage must be conducted to limit access to evidence outside the warrant," and (4) "conditions on when the seized hardware must

146. United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005).
147. OLE MANUAL, *supra* note 116, at 80.
148. Kerr, *supra* note 145, at 1245.
149. Brenner & Frederiksen, *supra* note 108, at 81–84, 114; Winick, *supra* note 9, at 102–14.
150. Kerr, *supra* note 145, at 1261–73.
151. 442 U.S. 319 (1979).
152. *Id.* at 326–28.
153. 441 U.S. 238 (1979).
154. *Id.* at 258–59.
155. 547 U.S. 90 (2006).
156. An anticipatory warrant is a warrant granted for a place where evidence of the crime is not yet present, but is expected to be present sometime in the future. *Id.* at 94. A "triggering condition," such as the delivery of contraband, is often included. *Id.* These are usually issued in the context of narcotics deliveries. Kerr, *supra* note 145, at 1267.
157. *Grubbs*, 547 U.S. at 97–98.
158. Kerr, *supra* note 145, at 1267–68.
159. *Id.*

be returned."[160] Limiting the search to certain keywords, as stated already and reiterated below, may be impractical because some files cannot be searched by keywords and files can be intentionally mislabeled, among other complications.[161] This particular complication is of utmost concern to the government in its rejection of an approach that imposes ex ante limitations to restrict its investigation.[162] Still, contrary to the government's arguments and suggestions,[163] magistrate judges have imposed restrictions where they feared abuse of the warrants they were issuing.[164]

3. The Execution of the Search

There are two basic stages to most computer searches: the data acquisition phase, where the investigator retrieves or copies items on the suspect's computer, and the data reduction phase, where the investigator takes the "image copy" of the hard drive and tries to tease out the desired evidence.[165] Courts are highly deferential to imaging an entire hard drive because more time is needed to sort through the complexities of a digital search.[166] Only the Ninth Circuit requires the reasons for such action to be particularly stated in a warrant.[167] This lenient time period allows for a much more extensive search and can be considerably more intrusive based on the thorough processes that are required.

Forensic software, such as "EnCase," is typically employed to assist in the execution of a computer search.[168] Searches with this software are conducted at both a "logical" and "physical" level.[169] The logical approach is conducted by searching for the particular type of file described in the warrant, such as an image. It will pull up all files that have extensions commonly associated with images, such as ".jpg." However, because users can change these extensions easily, the physical approach is necessary to locate files whose extensions have been altered by searching for "file headers" that cannot be changed.[170]

---

160. Kerr, *supra* note 145, at 1249.

161. OLE MANUAL, *supra* note 116, at 79.

162. *See infra* notes 335–38, 372–73 and accompanying text.

163. OLE MANUAL, *supra* note 116, at 80.

164. Kerr, *supra* note 145, at 1245.

165. OLE MANUAL, *supra* note 116, at 78. This process is also called "imaging" and "analysis." *Id.* at 86. Some suggest a third, intermediate stage "authentication" that involves making forensic matches between objects found on the computer and what was being sought in the warrant before examining it, a much more restrictive approach than is taken by most officers when searching computers. Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227, 1232–33 (2004).

166. OLE MANUAL, *supra* note 116, at 77.

167. *Id.*

168. *Id.* at 89. The OLE Manual also states that this has no effect on Fourth Amendment issues. *Id.*

169. Kerr, *supra* note 7, at 544–45.

170. *Id.*; *see* Michael, *supra* note 20, at 926 (explaining problems with mislabeling); *see also, e.g.*, United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010); United States v.

The process is similar for text files. The logical search is a first attempt to find the desired materials by pinpointing a search to where they might be expected to be found (such as by keyword, grouping, date, or author), and the physical search almost indiscriminately searches throughout the entire hard drive.[171] This process is exhaustive and intrusive, since an investigator will look at all files of a given type or header rather than limiting his search in a more cautious way. Furthermore, the searches for text files and for file headers can include an error rate to account for misspellings, thus returning results of completely unrelated items sharing a few letters with the desired item.[172]

Investigators can also search for files using a "hash"—a "complicated mathematical operation, performed by a computer on a string of data, that can be used to determine whether two files are identical."[173] Law enforcement organizations keep records of common hash values for certain files associated with crimes, most often child pornography.[174] Even using this method, suspects can encrypt files and the decryption process can be lengthy and often fruitless.[175] Thus, "hash" searches are less effective and never used exclusively. Faced with all these limitations in less intrusive search methods, magistrates and courts afford officers significant discretion. While seemingly necessary, this may tread too heavily on the underlying purpose of the Fourth Amendment—reducing the discretion of law enforcement officers. Law enforcement officers are essentially given authority to open whichever files they deem necessary to their investigation.[176]

4. The Practical Effects of Digital Search Methods

These search methods lead investigators to review copious amounts of materials on a computer, including a host of documents not included in the search warrant. Searching among commingled records is inevitable, and a cursory examination may be necessary.[177] Courts have found that in the context of physical searches, this should constitute a "brief perusal" of each document to determine if it falls within the scope of the warrant, and seizure of items outside the warrant can only occur if their incriminating nature is immediately apparent.[178] However, in digital searches, this brief perusal is much more intrusive.[179]

Williams, 592 F.3d 511, 523 (4th Cir. 2010); United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006).

171. Kerr, *supra* note 7, at 545–46.

172. *Id.* at 546.

173. *Id.* at 541; *see* Howard, *supra* note 165, at 1233–35.

174. *See* Kerr, *supra* note 10, at 546.

175. *Id.* at 546–47.

176. *See supra* note 113 and accompanying text; *infra* notes 204, 319 and accompanying text; *infra* Part IV.

177. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

178. *See* United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1981).

179. *See supra* Part II.B.3.

Nevertheless, courts have followed the reasoning used in physical cases to support perusing files on a computer.[180] Plain view in physical searches is easier to apply because of the intuitive distinction between what is hidden and what is exposed.[181] By applying it in the digital context, courts are affording law enforcement almost limitless discretion. A search warrant for a physical environment does not necessarily include all objects contained therein,[182] but again, this is exactly how many computer searches are conducted. While it may be true that "[t]here is no way to know what is in a file without examining its contents,"[183] that rationale is much less destructive in the context of a file cabinet where the documents therein are limited both in number and in the subject matter they likely contain. The practical difficulties inherent in these searches should not justify added deference to police officers.

III. CIRCUIT BOARDS AND SPLITS: THE CONFLICT OF APPLYING THE PLAIN VIEW EXCEPTION TO DIGITAL SEARCHES

Courts have struggled with how to apply the plain view exception to digital searches in light of the practical difficulties discussed above.[184] This part analyzes the varying interpretations of the problem among the circuits, and the differing opinion regarding whether to adopt new practices.

Part III.A explores the holdings of the circuits that adopt the traditionalist approach, as well as the circumstances of those cases, to highlight its potential for abuse. Part III.B discusses the approaches of the Ninth and Tenth Circuits, which have, to different degrees, suggested the imposition of ex ante limitations to help protect Fourth Amendment rights before they are violated.

A. 'RAM'ing a Square Peg into a Round Hole: The Traditionalist Approach

In two 2010 decisions, the Fourth and Seventh Circuits reacted to the changing tide of cases in both the Ninth and Tenth Circuits by adhering to the traditional application of the *Horton* three-prong test, and found that new technology did not justify new principles.[185] More recently, the Third Circuit followed the Fourth and Seventh Circuits, expressly rejecting the Ninth Circuit's prophylactic rules.[186] Several other courts have been similarly hesitant to depart from fundamental doctrines when faced with the

180. *See, e.g.*, United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007); Manno v. Christie, No. 08-3254, 2008 WL 4058016, at *4 (D.N.J. Aug. 22, 2008); United States v. Potts, 559 F. Supp. 2d 1162, 1175–76 (D. Kan. 2008); United States v. Fumo, No. 06-319, 2007 WL 3232112, at *6 (E.D. Pa. Oct. 30, 2007).

181. *See* Kerr, *supra* note 7, at 554.

182. *See id.* at 555.

183. United States v. Hill, 322 F. Supp. 2d 1081, 1090 (C.D. Cal. 2004).

184. *See supra* Part II.

185. *See* United States v. Mann, 592 F.3d 779, 785–86 (7th Cir. 2010); United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010).

186. United States v. Stabile, 633 F.3d 219, 233–34 (3d Cir. 2011).

needs of law enforcement in searching and seizing digital information.[187] They often find that limiting police discretion in these circumstances is unnecessary; search protocols will only assist criminals at the expense of effective investigation.[188] Several commentators agree that the Ninth Circuit's suggestions are excessive and improper, and that law enforcement is better served through adherence to the traditionalist approach.[189] Whatever their support, these sample cases display the tremendous discretion afforded to law enforcement in the execution of digital searches.

1. Fourth Circuit

In *United States v. Williams*,[190] the Fourth Circuit upheld the seizure of child pornography and weaponry found while executing a search relating to threatening messages sent to a Baptist elementary school.[191] The officer investigating the threats approached a magistrate for a warrant to search the defendant's home for evidence of crimes involving threats and vulgar communications made to schoolchildren.[192] To justify a computer search, the officer cited the nature of the communications, and that, in his experience, those engaged in the sexual exploitation of children keep documents and images related to these crimes on electronic storage devices.[193] The magistrate judge issued a search warrant authorizing the collection of "[a]ny and all computer systems and digital storage media, videotapes, videotape recorders, documents, photographs, and Instrumentalities indicat[ive] of the offense."[194] Pursuant to this warrant, the officers seized all electronic storage and media devices for a later search.

---

187. *See* United States v. Miranda, 325 F. App'x 858, 860 (11th Cir. 2009) (applying the plain view doctrine in a straightforward manner, likening computer files to intermingled documents, and finding that law enforcement has the right to search all files on any digital device it has a warrant to search); *Hill*, 322 F. Supp. 2d at 1090–91; Rosa v. Virginia, 628 S.E.2d 92, 94–97 (Va. Ct. App. 2006).

188. United States v. Hanna, No. 07-CR-20355, 2008 WL 2478330, at *6–7 (E.D. Mich. June 17, 2008) (rejecting the argument that a computer search should have been limited to particular search protocol because "[c]omputer files are easy to disguise or rename"); United States v. Maali, 346 F. Supp. 2d 1226, 1245–47 (M.D. Fla. 2004) (allowing a general search of all computer files and finding that the lack of a detailed search protocol is acceptable because it is not the scope, but the reasonableness of the search that matters constitutionally); Wisconsin v. Schroeder, 613 N.W.2d 911, 915–17 (Wis. 2000) (finding the search of all user-created files to be an acceptable way for police to look for evidence within the scope of the warrant).

189. *See, e.g.*, Kerr, *supra* note 145, at 1261–73; Vincent Angermeier, Comment, *Swinging for the Fences: How* Comprehensive Drug Testing, Inc. *Missed the Ball on Digital Searches*, 100 J. CRIM. L. & CRIMINOLOGY 1587, 1587 (2010); Scott D. Blake, Note, *Let's Be Reasonable: Fourth Amendment Principles in the Digital Age*, 5 SEVENTH CIRCUIT REV. 491, 493 (2010); Timothy C. Cedar, Note, *The Guidelines of* Comprehensive Drug Testing, Inc.*: A Measured Approach?*, 89 OR. L. REV. 351, 383 (2010).

190. 592 F.3d 511 (4th Cir. 2010).

191. *Id.* at 514.

192. *Id.* at 515.

193. *Id.*

194. *Id.* (alteration in original).

In the subsequent off-site search, an investigating agent reported that he had located "many deleted images" of child erotica,[195] and that anonymizer software had been installed.[196] The agent continued his search through all the suspect's electronic storage devices and found a DVD labeled "Virus Shield, Quarant[in]ed Files, Destroy" that contained child pornography.[197] Williams was charged with possession of child pornography and possession of an unregistered firearm.[198] After his conviction, Williams appealed the denial of his motion to suppress the pornography.[199] In his appeal, Williams argued that the police did not sufficiently limit their search when they searched every file on his computer.[200] He contended that allowing plain view in this context would "read . . . the warrant requirement out of the Fourth Amendment," and that the officers only used the warrant in his case as a vehicle for gaining access to the computer to search for evidence of child pornography that they suspected him of possessing from the outset of the search—meaning that the officers clearly had not stumbled across the files "inadvertently."[201]

The court, after recognizing that the purpose of the Fourth Amendment was to prevent general searches, stated that "some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."[202] The court held that the warrant gave the officers the authorization to "open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization."[203] Based on this conclusion that officers had a lawful right of access to every file, the three-prong *Horton* test was applied to find that the seized items were in plain view.[204] Finding the analogy to a file cabinet to be satisfactory, the court found "no reason to depart [from the traditional objective test] in the context of electronic files."[205] *Williams* affords investigators the broadest authority to search and seize evidence of crimes by allowing the plain view doctrine to apply as it does in physical searches, effectively permitting the search of every file.

195. *Id.* at 516. "Child erotica" is non-pornographic images of children, often used for sexual gratification. *Id.* at 515 n.1.

196. *Id.* at 516.

197. *Id.*

198. *Id.*

199. *Id.* at 517.

200. *Id.* at 518.

201. *Id.* This assertion of the previously invalidated inadvertency requirement is based upon *United States v. Carey*, 172 F. 3d 1268 (10th Cir. 1999), discussed *infra* Part III.B.1.

202. *Williams*, 592 F.3d at 519–20 (quoting Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976)).

203. *Id.* at 521.

204. *Id.* at 522.

205. *Id.* at 524.

2. Seventh Circuit

In *United States v. Mann*,[206] the Seventh Circuit expressly rejected the restrictive approach,[207] and found that it was more prudent to allow the doctrine to progress incrementally on the facts of individual cases, rather than abandoning the plain view doctrine in digital searches altogether.[208] Police received a tip that the defendant placed a secret video camera in a women's locker room.[209] A state prosecutor sought and received a broad warrant to search his home 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."[210] Officers executed the warrant and seized Mann's computer, laptop, and external hard drive before charging him with voyeurism.[211]

Officers did not search these devices until several months later.[212] The officers created a copy of each hard drive and then used software called "forensic tool kit" (FTK)[213] to catalog the contents of the computer by creating a list of all "known file formats" (KFF Alert) on a hard drive.[214] KFF Alert flags files previously submitted by law enforcement, most of which are child pornography.[215] After searching through the flagged files and others, the officers found a significant amount of child pornography and several videos of the female locker room in question.[216] The district court denied Mann's motion to suppress the child pornography because they found it within the scope of the warrant for the officer to search all the files on the computer.[217] Mann entered a conditional guilty plea and argued on appeal that the use of the FTK software and KFF filter to locate images of child pornography when the warrant authorized the collection of digital media evidencing recordings of women in locker rooms and public places was impermissible.[218]

The *Mann* court first noted the inherent problem of limiting computer searches where evidence "could be nearly anywhere on . . . [a] computer[]" because of "manipulat[ion] to hide [file] contents."[219] When the officer testified at the suppression hearing, he stated that he "'would search in all the files if [he] felt it necessary . . . [or] pertinent to [his] case.'"[220] The

206. 592 F.3d 779 (7th Cir. 2010).
207. *See infra* Part III.B.
208. *Mann*, 592 F.3d at 785.
209. *Id.* at 780.
210. *Id.* at 780–81.
211. *Id.* at 781.
212. *Id.*
213. *Id.* FTK software creates a list of all files on a computer to let an officer know how many files of each format (documents, images, etc.) are present on a hard drive, and indicates whether they are encrypted or not, among other functions. *Id.*
214. *Id.*
215. *Id.*
216. *Id.*
217. *Id.* at 781–82.
218. *Id.* at 782–83.
219. *Id.* at 782.
220. *Id.* at 783.

court found that the use of the FTK software was acceptable even though it flagged files containing evidence of crimes not listed in the warrant because officers must be able to look for evidence "virtually anywhere on [a] computer[]."[221] As to the four "flagged 'KFF Alert' files," the court found that once they were flagged, the officer "knew (or should have known)" that files in the database containing these known child pornography issues would be outside the warrant, but deemed it harmless error, as ample evidence existed from a previous search.[222]

The court held that it "believe[d] the more considered approach would be to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication," and simply urged "caution" in following the Fourth Amendment's requirements in these cases.[223] This traditional approach approved of the broad search of nearly all files on a computer and approved the officer's statement that he found it in his discretion to do so.

3. Third Circuit

In *Stabile v. United States*,[224] the defendant wrote over $150,000 in counterfeit checks to maintain a mortgage he defaulted on before being investigated.[225] Upon learning of his counterfeit checks, Secret Service Special Agents Albanese and Croes traveled to Stabile's home to gather information.[226] Upon arrival, they requested his wife's consent to a search of their home, which she granted.[227] The officers discovered physical evidence adjacent to Stabile's computer that they believed related to the alleged bank fraud.[228] The agents called the local prosecutor's office, which sent over computer crimes specialists to disconnect the hard drive.[229] In the course of their search, the agents also found DVDs that they believed contained child pornography. However, upon examination they were found to be innocuous.[230]

Once in possession of the hard drives, the agents did not apply for a state search warrant until almost three months later.[231] The warrant they received authorized a search for evidence of bank crimes as well as child

221. *Id.* at 784. *But see CDT II*, 579 F.3d 989, 999 (9th Cir. 2009) (finding that use of such software to locate well-known illegal files may not be used without specific authorization in the warrant).

222. *Mann*, 592 F.3d at 784–85. While at least one commentator has called this approach unique, *see* Kerr, *supra* note 16, it essentially imposes no significant limitations on an officer's discretion, and thus will be deemed "traditionalist" for purposes of this Note.

223. *Mann*, 592 F.3d at 785–86 (quoting *CDT II*, 579 F.3d at 989 (Callahan, J., concurring in part and dissenting in part)).

224. 633 F.3d 219 (3d Cir. 2011).

225. *Id.* at 224.

226. *Id.*

227. *Id.* at 224–25.

228. *Id.* at 225.

229. *Id.*

230. *Id.* at 226.

231. *Id.* The agents' proffered reason for this was that one of them was busy on a presidential detail. *Id.*

pornography, despite the fact that no probable cause existed after local law enforcement had reviewed the DVDs and found no evidence.[232] The agents learned of this error and instructed the computer crimes specialist, Detective Vanadia, to stop searching and contact the Secret Service if he came across evidence of crimes other than bank fraud.[233]

While reviewing the evidence, Vanadia highlighted a folder with the label "Kazvid." The detective testified that it was associated with the peer-to-peer network Kazaa,[234] which he explained is often used to transfer child pornography.[235] The detective "highlighted" the folder—a process that allowed him to view the file names inside—and found several video files with suggestive titles.[236] The court noted that "although Vanadia admitted that he . . . did not believe these video files contained evidence of financial crimes, Vanadia proceeded to open twelve different video files . . . to 'confirm' that they contained child pornography."[237] After discovering child pornography, the officer contacted Agent Albanese and the local prosecutor's office.[238]

Agent Albanese then received a federal search warrant for child pornography based upon the file names viewed in the Kazvid folder.[239] This did not mention that Detective Vanadia had actually opened the files.[240] After conducting the search and seizing the child pornography, Stabile was arrested and indicted for bank fraud and receipt of child pornography.[241] The district court denied Stabile's motion to suppress, rejecting his argument that Vanadia exceeded the scope of the warrant on the basis of the inevitable discovery and independent source doctrines.[242] The judge convicted Stabile in a bench trial with several stipulations, among them the right to appeal the suppression motion.[243]

On appeal, Stabile challenged his conviction on myriad Fourth Amendment issues. Among those was the scope of the plain view doctrine as it applied to Detective Vanadia's search.[244] While Stabile argued that even the file names inside the Kazvid folder were not in plain view, the

232. *Id.*
233. *Id.* at 226–27.
234. Peer-to-peer networks allow users to share files over a network without a central server. *Id.* at 227.
235. *Id.*
236. *Id.*
237. *Id*.
238. *Id.*
239. *Id.*
240. *Id*. at 227–28.
241. *Id.* at 228.
242. *Id.* at 228–29. The independent source doctrine is an exception to the exclusionary rule that allows admission of "evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality." Murray v. United States, 487 U.S. 533, 537 (1988). The inevitable discovery doctrine allows otherwise tainted evidence to be admitted if "the information ultimately or inevitably would have been discovered by lawful means." Nix v. Williams, 467 U.S. 431, 444 (1984).
243. *Stabile*, 633 F.3d at 230.
244. *Id.* at 237.

government argued that the contents of those files were appropriate to search.[245] The Third Circuit affirmed the district court's holding and reasoning.[246] Rejecting the argument that Detective Vanadia knew that the Kazvid folder likely would not contain evidence of bank fraud, the court cited the usual difficulties posed by mislabeling, and the fact that subjective intent of the officer is irrelevant.[247] They found that after using limited search methods, "examin[ing] suspicious and out-of-place folders, such as the Kazvid folder" was proper.[248] The court found a search of all the file names in the Kazvid folder reasonable, and left open the question of viewing their contents.[249] This ambiguity leaves open the possibility that there are no limitations on what an officer may view on a computer. The Third Circuit expressly rejected the Ninth Circuit's suggestion to "forswear reliance on the plain view doctrine," finding the "more considered approach" would allow the doctrine to develop incrementally.[250]

B. Tough Times Call for Prophylactic Measures: The Restrictive Approach

Unlike the traditionalist view, circuit courts that suggest the restrictive approach have resisted deferring entirely to the inherent difficulties in executing digital searches. The Ninth and Tenth Circuits, to different degrees, advocate a "higher" particularity standard[251] where computer warrants are used to restrict the wide discretion otherwise afforded to officers executing digital searches. Many scholars agree that digital searches pose troubling issues to Fourth Amendment protections, and the Ninth Circuit's prophylactic measures were at least a step in the right direction.[252] Critics, while not always believing that the traditionalist approach is best, challenge the legitimacy of placing restrictions on the execution of searches as being unwise, constitutionally impermissible, or in direct conflict with the Federal Rules of Criminal Procedure.[253]

245. *Id.*
246. *Id.*
247. *Id.* at 239–40.
248. *Id.* at 240.
249. *Id.* at 242.
250. *Id.* at 241 n.16.
251. This Note argues that prophylactic rules similar to those suggested by the Ninth Circuit are not imposing a "higher" standard, but doing no more than adhering to the particularity requirement. *See infra* Part IV.B.4.
252. *See, e.g.*, Michael, *supra* note 20 at 927–28; David H. Angeli et. al, *The Plain View Doctrine and Computer Searches: Balancing Law Enforcement's Investigating Needs with Privacy Rights in the Digital Age*, CHAMPION, Oct. 2010, at 18, 23; Bryan K. Weir, Comment, *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, 121 (2010).
253. *See, e.g.*, Kerr, *supra* note 145, at 1261–73; Moshirnia, *supra* note 123 at 626–35.

1. Tenth Circuit

In *United States v. Carey*,[254] the Tenth Circuit found that child pornography discovered in the execution of a search warrant for other crimes was not in plain view because the officer knew he expanded the scope of the warrant by abandoning his search for drugs to search for child pornography.[255] While executing a warrant for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances,"[256] the investigating officer observed several sexually suggestive titles with a label commonly associated with images.[257] The officer admitted he had never encountered a situation where such labels were used to disguise the sort of documentary evidence he was seeking.[258] "Undaunted," he "explore[d] the directories and encountered some files he 'was not familiar with.'"[259] The officer did not obtain a second warrant, but believed that he "had to search these files as well as any other files contained [on the computer]."[260] After discovering child pornography in these files, the defendant was convicted for their possession.[261]

After his conviction, the defendant appealed on the grounds that the search conducted by the investigating officer "transformed the warrant into a 'general warrant' and resulted in a general and illegal search of the computers and their files."[262] The government contended that the search of a computer was comparable to a file cabinet and the common concerns about mislabeling.[263]

The court found that after the investigating officer opened the first image file and discovered child pornography, he continued his search expecting to find more of the same.[264] Under these circumstances, the court found that the discovery of these images was therefore not "inadvertent[],"[265] and he had conducted an "unconstitutional general search."[266] It further stated that the comparison to a file cabinet was inappropriate and that the enormous amount of intermingled data present on computers necessitates the "intermediate step of sorting various types of documents and then only search[ing] the ones specified in a warrant."[267] The court instructed that

254. 172 F.3d 1268 (10th Cir. 1999).
255. *Id.* at 1274.
256. *Id.* at 1270.
257. *Id.*
258. *Id.* at 1270 & n.2.
259. *Id.* at 1271.
260. *Id.* (alteration in original).
261. *Id.* at 1270.
262. *Id.* at 1271–72.
263. *Id.*
264. *Id.* at 1273.
265. *Id.* While inadvertence as an element for the plain view doctrine was eliminated in *Horton v. California*, *see supra* note 100 and accompanying text, the court based its findings on the fact that the officer knew he was going outside the scope of the search. *Carey*, 172 F.3d at 1273.
266. *Id.* at 1276.
267. *Id.* at 1274–75.

officers should have to seek a magistrate's approval on specific limitations to protect Fourth Amendment rights.[268] The court further found that because the officers had seized the computer and searched it off-site, there was no reason to rummage through all the files without sticking to a narrow search to find the information specified in the warrant.[269]

The Tenth Circuit's opinion in *Carey* arguably deserves a unique designation as a subjective test, recognizing that "inadvertence is a characteristic of most legitimate 'plain-view' seizures" and was thus "certainly relevant to [the] inquiry."[270] However, the court noted its findings were fact intensive,[271] and many courts distinguish *Carey* based on these grounds.[272] Subsequently, the Tenth Circuit has interpreted the opinion to raise the particularity standard of warrants for digital evidence, where files are so intermingled as to necessitate limitations.[273] *United States v. Walser*[274] held that "when officers come across relevant computer files intermingled with irrelevant computer files, they 'may seal or hold' the computer 'pending approval by a magistrate of the conditions and limitations on a further search' of the computer."[275] It further held the "underlying premise in *Carey* is that officers conducting searches (and the magistrates issuing warrants for those searches) cannot simply conduct a sweeping, comprehensive search of a computer's hard drive."[276] In *United States v. Riccardi*,[277] the court found a warrant lacked the specificity required by *Carey* and its progeny where the warrant did not contain "as much specificity as the government's knowledge and circumstances allow."[278] However, the court, while finding that the use of search methodologies is proper and sometimes necessary, did not require search methodologies to be crafted in all cases it reviews for the search to be found reasonable.[279]

268. *Id.* at 1275.
269. *Id.* at 1275–76.
270. *Id.* at 1277 (this statement was made in the court's order on petition for rehearing).
271. *Id.* at 1276.
272. *See, e.g.*, United States v. Mann, 592 F.3d 779, 783 (7th Cir. 2010); United States v. Giberson, 527 F.3d 882, 890 (9th Cir. 2008); United States v. Fiscus, 64 F. App'x 157, 163–64 (10th Cir. 2003).
273. *See, e.g.*, United States v. Burgess, 576 F.3d 1078, 1092–94 (10th Cir. 2009) (explaining that *Carey* attempted to encourage the use of limitations on search warrants, pointing to the dicta that "suggested methods to constrain searches, keying on the type of files identified in the warrant, file names, key word searches, directory structure," yet still finding that such restrictions, at least in the case at hand, would be "folly").
274. 275 F.3d 981 (10th Cir. 2001).
275. *Id.* at 986 (quoting *Carey*, 172 F.3d at 1275).
276. *Id.*
277. 405 F.3d 852 (10th Cir. 2005).
278. *Id.* at 863.
279. *See, e.g.*, United States v. Burke, No. 10-3030, 2011 WL 310520, at *8 (10th Cir. Feb. 2, 2011); United States v. Burgess, 576 F.3d 1078, 1092–93 (10th Cir. 2009).

2. Ninth Circuit

Where the Tenth Circuit stopped short, the Ninth Circuit pressed forward. In *United States v. Comprehensive Drug Testing, Inc.* (*CDT II*), a limited en banc panel of the Ninth Circuit initially mandated that officers waive reliance on the plain view doctrine in digital searches and follow a set of prophylactic rules designed to protect Fourth Amendment rights.[280] This ruling led to an appeal by then-Solicitor General Elena Kagan and twenty-two other federal attorneys for a full en banc rehearing to reconsider what they found to be "sweeping new rules for warrants to search computers that are having an immediate and detrimental effect on law enforcement efforts."[281] The court eventually decided to revise its opinion, making these "sweeping new rules" a safe haven and limited its holding to a test that asks the judiciary to employ "greater vigilance" in striking the correct balance between private and governmental interests in digital searches (*CDT III*).[282]

United States v. Comprehensive Drug Testing, Inc. involved three cases consolidated on appeal stemming from the government's investigation of the Bay Area Lab Cooperative (BALCO). BALCO allegedly distributed illegal steroids to Major League Baseball (MLB) players.[283] The government began investigating BALCO in August 2002 and eventually gathered enough evidence to believe at least ten MLB players had received drugs from BALCO.[284] The government was aware that MLB and the Major League Baseball Players Association (MLBPA) had entered into a collective bargaining agreement in which the players consented to anonymous and confidential drug testing solely to let MLB determine the magnitude of steroid use to fashion any necessary policies.[285] As part of the BALCO investigation, the government served MLB with a subpoena requesting the test results of eleven players that had connections with BALCO.[286] MLB denied that they were in possession of those records.[287]

The government then subpoenaed third-party drug test administrators of Comprehensive Drug Testing (CDT) and Quest for drug testing information relating to all MLB players.[288] After CDT and Quest continuously challenged the scope of the subpoena, the government served them with a new subpoena modified to request only the tests of ten of the eleven MLB players initially under investigation.[289] After the MLBPA continued to

280. *CDT II*, 579 F.3d 989, 1006 (9th Cir. 2009).
281. Eddlem, *supra* note 17.
282. *CDT III*, 621 F.3d 1162, 1177 (9th Cir. 2010).
283. United States v. Comprehensive Drug Testing, Inc. (*CDT I*), 513 F.3d 1085, 1089 (9th Cir. 2008).
284. *Id.*
285. *Id.* at 1118 (Thomas, J., concurring in part and dissenting in part).
286. *Id.* at 1090 & n.7 (majority opinion).
287. *Id.* at 1090.
288. *Id.*
289. *Id.* at 1090 & n.7.

challenge the subpoenas, the government obtained warrants to search both laboratories for evidence relating to the BALCO investigation.[290]

The original warrants, issued on April 7, 2004, authorized the seizure of the records of the ten BALCO-related MLB players listed in the subpoena, as well as materials "detailing or explaining" CDT or Quest's "administration of Major League Baseball's drug testing program."[291] The warrants authorized investigators to copy and search electronic files off-site.[292] It directed that "computer personnel"[293] choose the best course to capture the data sought, and "appropriately trained personnel" would review and segregate the relevant data, returning anything outside the scope of the warrant.[294] Furthermore, the search of such intermingled records and entries in directories in the Ninth Circuit must comply with the procedures outlined in *United States v. Tamura*[295] for the segregation of physical evidence.

On April 8, 2004, the government executed both the CDT and the Quest warrants. Twelve federal agents entered the CDT laboratory and seized the "Tracey" directory containing all of the computer files for the sports drug-testing program.[296] Back at his office, the primary case agent conducted the search over objections from CDT's legal counsel, who had requested that a magistrate or special master conduct the investigation.[297] The agent found five sub-directories related to MLB, as well as items authorized for seizure in the warrant, including the master list of positive test results.[298] The Quest warrant was executed the same day.[299] Though the original warrants only provided for the seizure of the records of the ten players for which there existed probable cause, the investigators gained access to the test results of all the players in the anonymous testing.[300]

After this broad search of the "Tracey" directory, the government pursued authorization to seize all records pertaining to its investigation, including the test results of all players.[301] Between April 30 and May 6 of 2004, investigators obtained warrants and subpoenas in three separate districts (District of Nevada, and the Central and Northern Districts of California) that allowed for broad seizure of all electronic records.[302] After their execution, CDT sought return of the records in the three districts in which magistrates had granted the warrants and subpoenas.[303] Judges

290. *Id.* at 1091.
291. *Id.*
292. *Id.* at 1092–93.
293. *Id.* at 1093. The warrant defined computer personnel as "law enforcement personnel trained in searching and seizing computer data." *Id.* at 1092 (internal quotations omitted).
294. *Id.*
295. 694 F.2d 591 (9th Cir. 1982).
296. *CDT I*, 513 F.3d at 1092.
297. *Id.* at 1120–21 (Thomas, J., concurring in part and dissenting in part).
298. *Id.* at 1093 (majority opinion).
299. *Id.*
300. *Id.* at 1093–94.
301. *Id.* at 1094.
302. *Id.* at 1093 n.20, 1099.
303. *Id.* at 1094.

James Mahan, Susan Illston, and Florence-Marie Cooper all condemned the government's practices in their decisions on these motions.[304]

In his order to return the evidence seized under the Nevada warrant (the Mahan Order), Judge Mahan found that the government "callously disregarded the affected players' constitutional rights" and failed to follow procedures set forth in *United States v. Tamura*[305] pertaining to the search of intermingled records.[306] Judge Cooper similarly criticized the government's failure to follow *Tamura* in her order to return the evidence seized under the warrant granted in the Northern District of California (Cooper Order).[307] Judge Illston went so far as to call the government's actions unreasonable and evidence of harassment in quashing the subpoenas in question (Illston Quashal).[308]

The government appealed these three decisions, which were considered together by the Ninth Circuit. In January of 2008, after vacating a previous decision, a three-judge panel affirmed the Mahan Order, but reversed the Cooper Order and the Illston Quashal, finding that the government acted reasonably.[309] The Ninth Circuit granted a petition to rehear the case en banc. Part III.B.2.a evaluates the limited en banc rehearing that created a set of prophylactic rules adopted from *Tamura* to protect Fourth Amendment rights in the execution of computer search warrants.[310] Part III.B.2.b outlines the reaction to this opinion by the government and other courts, while also detailing the revised opinion[311] that removed the binding effect of the original protective measures outlined in *CDT II*.

a. CDT II and the Prophylactic Rules Described Therein

Several months after the issuance of the 2008 decision, all active, non-recused judges granted a motion for a limited en banc hearing of the issues presented upon appeal.[312] The en banc panel of eleven judges reconsidered the original panel's findings on each of the orders while "tak[ing] the opportunity to guide [their] district and magistrate judges in the proper administration of search warrants and grand jury subpoenas for electronically stored information."[313]

The court first determined that the Cooper Order was binding because the government failed to appeal those findings in a timely manner.[314] The court found that the evidence ordered returned by Judge Cooper, while seized under a broad warrant based on a general concern about the inability

304. *Id.* at 1094–95 & n.20; *id.* at 1125–27 (Thomas, J., concurring in part and dissenting in part).
305. 694 F.2d 591 (9th Cir. 1982).
306. *CDT I*, 513 F.3d at 1094.
307. *Id.* at 1125–27 (Thomas, J. concurring in part and dissenting in part).
308. *Id.* at 1095 (majority opinion).
309. *Id.*
310. *CDT II*, 579 F.3d 989 (9th Cir. 2009).
311. 621 F.3d 1162 (9th Cir. 2010).
312. United States v. Comprehensive Drug Testing, 545 F.3d 1106 (9th Cir. 2008).
313. *CDT II*, 579 F.3d at 994.
314. *Id.* at 994.

to efficiently segregate information, "wisely" contained restrictions on the methods of search and seizure—restrictions that the government "completely ignored."[315] The court also mentioned the binding effect of the Illston Quashal that necessarily rejected the government's arguments about the scope of the warrant.[316]

The court, having established the preclusive effects of these findings, moved on to the panel's reversal of the Mahan Order. The en banc panel supported Judge Mahan's findings that "the government callously disregarded the affected players' constitutional rights" and failed to follow the guidelines contained in *Tamura*.[317] The panel rejected the government's argument that it had followed *Tamura* because any other player's positive test results were discovered pursuant to the plain view doctrine.[318] As to the proper scope of the plain view doctrine, the court found: "If the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file—and we have no cavil with this general proposition—then everything the government chooses to seize will, under this theory, automatically come into plain view."[319] When this problem is presented, the court first suggested that investigators "forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data."[320] The court also mandated that the method chosen to search data must be designed to find that which is seizable and only that—a goal that could be accomplished by complex hashing tools as outlined earlier.[321]

The court also criticized the government's failure to use "computer personnel" in the initial review of the seized data, rather than allowing the primary case agent to do it himself.[322] The specialist did nothing to segregate the data after making his initial determination that the data could not be sorted on-site.[323] The court found it necessary to instruct that, in warrants for such a broad amount of data, there should be a protocol preventing agents engaged in the investigation from examining or retaining any data other than that for which there is probable cause.[324]

The majority then moved on to consider the Illston Quashal, finding that Judge Illston had not abused her discretion in quashing the subpoenas issued after the Cooper and Mahan Orders.[325] It established that it is not per se unreasonable to seek both a subpoena and a warrant for the same

315. *Id.* at 995–96.
316. *Id.* at 997.
317. *Id.*
318. *Id.*
319. *Id.* at 998.
320. *Id.*
321. *Id.* at 999; *see also supra* Part II.B.3.
322. *CDT II*, 579 F.3d at 999.
323. *Id.* at 1000.
324. *Id.* at 999.
325. *Id.* at 1003–04.

investigation.[326] Yet, when applying for any sort of investigatory tools, law enforcement must make clear to any judicial officer any prior attempts to obtain such information in other fora.[327]

Upon conclusion of the consideration of the appeals of the case, the court outlined the reasoning behind its findings and discussed the underlying constitutional issues presented by digital searches. It found that digital searches pose a fundamental Fourth Amendment issue that was not easily resolved by analogy to previous jurisprudence: "Th[e] pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[328] Because authorization to search some computer files "automatically" becomes a license to search all files within a given directory, hard drive, or other expansive collection, the court found it necessary to emphasize its holding by outlining procedures, adapted from its previous *Tamura* decision, to be followed by magistrates in digital search cases to avoid Fourth Amendment violations:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
>
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
>
> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.[329]

The court concluded by emphasizing that we must "rely on the good sense and vigilance of our magistrate judges" to protect Fourth Amendment rights in this regard.[330] As opposed to the traditionalist approach,[331] these prophylactic rules shift the focus from ex post review to the warrant application process to prevent general searches before they inevitably occur. The court found that the peculiar and difficult complications involved in

326. *Id.* at 1003.
327. *Id.* at 1004.
328. *Id.*
329. *Id.* at 1006.
330. *Id.* at 1007.
331. *See supra* Part III.A.

computer searches necessitated a radically different approach to prevent Fourth Amendment violations.

b. The Reaction and the Revised Opinion (CDT III)

The prophylactic rules created in *CDT II* met a considerable amount of resistance following their creation. While some courts accepted these restrictions to certain degrees,[332] courts considering the issue more often rejected these new rules, including the *Williams* and *Mann* decisions discussed above.[333] A district court within the Ninth Circuit even distinguished *CDT II* on the basis that it involved a case where the court was primarily concerned with deliberate overreaching by the government and refused to find the directives contained therein to be binding.[334]

The executive's response to the decision was immediate and highly critical. Then-Solicitor General Elena Kagan filed a petition on November 23, 2009 for a full en banc rehearing of all twenty-seven judges of the Ninth Circuit.[335] The government claimed that the en banc panel's decision had an "immediate and detrimental effect on law enforcement . . . . [and] [i]n some districts, computer searches [had] ground to a complete halt."[336] They posited that imposing these guidelines was beyond the scope of the present controversy, and that a better course for protecting Fourth Amendment rights would be to continue to allow courts to form rules piece by piece through the resolution of actual controversies.[337] To further its point, the government also put forth a parade of horribles about how the "filter team" requirement was unworkable and would result in the destruction of critical evidence.[338]

Nine months later, while refusing to rehear the case, the Ninth Circuit responded to the petition and revised its previous opinion, deeming it the "final action of the court."[339] As revised, the court backed away from its previously far-reaching holding, and narrowed its implications considerably. The previous 9-2 majority opinion was re-labeled "per curiam," and the portions that the government found offensive, including the prophylactic rules, were moved into a concurrence joined by only five

332. *See, e.g.*, United States v. Seldon, 385 F. App'x 676, 677–78 (9th Cir. 2010); Chaim v. United States, 692 F. Supp. 2d 461, 469 (D.N.J. 2010); United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *6 (D. Me. Dec. 3, 2009).

333. United States v. Mann, 592 F.3d 779, 784–85 (7th Cir. 2010); United States v. Williams, 592 F.3d 511, 524 (4th Cir. 2010).

334. United States v. King, 693 F. Supp. 2d 1200, 1229 (D. Haw. 2010).

335. Brief for the United States in Support of Rehearing En Banc by the Full Court, United States v. Comprehensive Drug Testing, Nos. 05-10067, 05-15006, 05-55354 (9th Cir. Nov. 23, 2009), *available at* https://ecf.ca9.uscourts.gov/cmecf/servlet/TransportRoom?servlet=CaseSummary.jsp&caseNum=05-55354&incOrigDkt=Y&incDktEntries=Y.

336. *Id.* at 1.

337. *Id.* at 1–8.

338. *Id.* at 15–18.

339. *CDT III*, 621 F.3d 1162, 1165 (9th Cir. 2010).

judges.[340] The language about guiding magistrate judges was moved to this concurrence,[341] and strong wording about the "illogical result" of allowing practical concerns to justify an overbroad warrant that allows whatever investigators choose to seize on a computer to come into plain view was completely removed.[342]

The previous mandates that the court provided to magistrate judges were now only "guidance"—a "safe harbor" of sorts—yet still designed to "protect[] the people's right to privacy and property in their papers and effects."[343] Thus, the binding guidance that emerged from the revised opinion was simply that the circumstances of computer searches "call[] for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures."[344] Despite this limited holding, the court retained much of its language explaining how the digital search context poses difficulties that will necessitate that a new "fair balance" be struck.[345] The per curiam opinion still points to the prophylactic rules now listed in the concurrence, admonishing that "clear rules" benefit all parties' interests.[346] The spirit of the previous opinion remained in the revised version: "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."[347]

IV. A NEW REGIME FOR DIGITAL SEARCHES IS NECESSARY TO COUNTER THE DANGER POSED TO THE UNDERLYING PRINCIPLES OF THE FOURTH AMENDMENT

The proliferation of the means and methods by which data is transmitted and stored has caused a strain on Fourth Amendment principles. The Fourth Amendment's reference to "papers" and "effects" is inapplicable in an environment where technology has significantly changed the way we live. Many courts have set aside the original principles and motivations underlying the Fourth Amendment when evaluating the plain view doctrine as applied to digital searches. Part III of this Note outlined the spectrum of opinion among the Courts of Appeals on this issue. Courts are hesitant to fundamentally depart from previous Fourth Amendment principles and doctrines in digital searches.[348] Judges are prone to "throw up their hands" when faced with the difficult obstacles presented to law enforcement and

340. *Id.* at 1178–80 (Kozinski, J., concurring).
341. *Id.* at 1180.
342. *Compare CDT II*, 579 F.3d 989, 998 (9th Cir. 2009), *with CDT III*, 621 F.3d at 1178–79.
343. *CDT III*, 621 F.3d at 1178.
344. *Id.* at 1177.
345. *Id.*
346. *Id.*
347. *Id.*
348. *See, e.g.*, *supra* note 328 and accompanying text.

permit a loosening of Fourth Amendment standards.[349] The motivations that prompted resistance to general warrants prior to the Fourth Amendment's drafting[350] should compel courts today to resist the current government's demand for wide discretion. Rather than sacrificing the original spirit of the Fourth Amendment by allowing digital searches to be conducted with such wide discretion, the judiciary should follow its "long and celebrated tradition" of "generalizing from those specific practices [that motivated the Fourth Amendment's drafting] to . . . broader evils," and find that changed circumstances in digital searches require a new set of rules.[351]

Natural rights involving privacy and freedom from unreasonable and arbitrary government action are inherent in the foundations of Anglo-American society.[352] The Fourth Amendment is the only procedural safeguard to derive directly from the events that preceded the American Revolution[353]—the abusive practices and unfettered discretion enjoyed by the government under the general warrants and writs of assistance in both England and the colonies.[354] This history continues to animate Fourth Amendment decisions,[355] and the Supreme Court has several times emphasized that "the 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."[356] This direction and attention to the spirit of the Fourth Amendment should guide courts in creating a new set of rules to govern cases involving digital evidence where general searches are unavoidable.[357]

As discussed below, a traditional application of the plain view exception in computer searches cannot be reconciled with the inherent problems that are present in the execution of warrants for digital data. A new scheme is needed and the previously binding prophylactic factors laid out in *CDT II* deserve attention as the approach that most protects the original meaning and spirit of the Fourth Amendment. Part IV.A discusses why the traditionalist approach is insufficient and why such a drastic change is both necessary and permissible. Part IV.B proposes prophylactic measures very similar to those contained in *CDT II*, and discuss how each is necessary to prevent the exercise of unfettered discretion by the government when conducting digital searches.

---

349. Michael, *supra* note 20, at 926–27.

350. *See supra* notes 46–47 and accompanying text.

351. *See* David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1813 (2000); *see also supra* notes 68–69 and accompanying text.

352. NEWMAN, *supra* note 52, at 11.

353. 1 LAFAVE, *supra* note 5, § 1.1(a); *see supra* notes 37–52.

354. *See, e.g.*, Davies, *supra* note 24, at 575–90; Maclin, *supra* note 28, at 218–29.

355. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31–32 (2001); Atwater v. City of Lago Vista, 532 U.S. 318, 336–40 (2001); Wilson v. Arkansas, 514 U.S. 927, 932–36 (1995).

356. *See* Horton v. California, 496 U.S. 128, 136 (1990); Arizona v. Hicks, 480 U.S. 321, 328 (1987); Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).

357. *See supra* notes 139–41, 319 and accompanying text.

A. The Suitability and Necessity of a New Scheme for Digital Cases to Protect Against Unreasonable Dragnet Searches

Recognition of the threat posed to Fourth Amendment rights by the inherent differences between physical and digital searches that allow for abusive dragnet searches should counsel the abandonment of the traditionalists' straightforward ex post application of the *Horton* three-prong test and the adoption of a new set of rules. Part IV.A.1 discusses why this test is fundamentally flawed in digital searches, and how the warrant application process exacerbates the problem. Part IV.A.2 discusses why the traditionalist approach fails. Part IV.A.3 proffers that the imposition of prophylactic rules is both constitutionally permissible and important.

1. The Flawed Traditionalist Ex Post Review and Practices of Law Enforcement

The *Horton* three-prong test is stretched beyond its bounds in ex post review of digital searches, and the practices of law enforcement do not comport with the plain view exception's original justifications. The first prong—that investigators are legally within the place where the incriminating objects can be seen—will always be present because warrants afford wide discretion to law enforcement officials to open files with innocuous labeling.[358] This assumption also satisfies the second prong by granting investigators a lawful right to access the object.

The most serious issues arise when examining the third prong—whether the incriminating nature of the evidence was "immediately apparent."[359] The plain view exception grew out of the inherent practicality and reasonableness that an officer should not have to obtain an additional warrant for objects that would be seizable upon view in a public place without a warrant.[360] But the incredible amount of data that can be stored on digital devices and the broad authority granted to investigators removes any reasonableness in considering every file in a digital storage device to be "out in the open."

Assuming that at least all file names on a computer are "in plain view," viewing the contents of such files surely involves an inspection not considered by past precedent because of what officers have to do to open or view them. Decoding and opening files involves a depth of investigation not permissible in physical searches.[361] The Supreme Court has commanded that the cursory inspection of innocuous paper documents must be a "truly cursory inspection—one that involves merely looking at what is

358. *See supra* notes 139–41, 193–94, 210, 301–05 and accompanying text.
359. *See supra* Part II.B.4.
360. *Arizona v. Hicks*, 480 U.S. 321, 324–25 (1987); *see supra* Part II.B.4.
361. *Cf. Hicks*, 480 U.S. at 326–27 (finding stolen property excludable on the basis that the investigating officer moved a stereo to view its serial numbers upon mere suspicion that it was stolen and it was thus not in "plain view").

already exposed to view, without disturbing it."[362] Courts have found that deeper inspection removes the immediately incriminating nature of items claimed to be in plain view.[363] In computer searches, investigators must take multiple steps to reveal what eventually may be deemed incriminating in files that are compressed, encrypted, deleted, or password protected.[364] These fundamental flaws in applying the three-prong test laid out in *Horton* should compel dispensing with this doctrine in the context of computer searches.

The procedures involved in the application and execution of digital search warrants exacerbate the problems present in ex post review.[365] Another practical justification for the plain view exception—the inconvenience of obtaining a second warrant and the risks to officers or evidence[366]—does not apply to computer searches where large scale copying occurs and officers are afforded ample time to search. Furthermore, in applying for the initial warrants, form language is often employed in affidavits supporting an officer's application. This language cites general concerns about the volume of information and the possibility of camouflage to justify authorization to search all items.[367] The warrants will rarely possess information that limits the search to particular circumstances of an individual investigation, such as limitations on the type of files sought (images, text, etc.), and do not specify why a blanket search of all files is necessary in any particular case.[368]

The government's professed policy reflects this acceptance of form language. The U.S. Department of Justice (DOJ) has shifted away from Fourth Amendment concerns toward maximizing an investigator's discretion. Originally, the DOJ took the position that despite the difficulties involved in digital searches, "agents cannot simply establish probable cause, describe the files they need, and then 'go' and 'retrieve' the data. Instead, they must understand the technical limits of different search techniques [and] plan the search carefully."[369] The first DOJ guide on searching and seizing computers contained concerns about limiting warrants to make sure they did not become too general and thereby unconstitutional,[370] with particular attention paid to the dangers posed to business records—advice that would have well suited the agents in

362. *Id.* at 328.

363. *See, e.g.*, *id.* at 326–27 (holding that the moving of stereo equipment to view serial numbers to determine if it was stolen constituted a separate search such that the stereo could not have been immediately incriminating); People v. Rivas, 626 N.Y.S.2d 640, 641 (N.Y. App. Div. 1995) (holding that when an officer had to piece together ripped sheets of paper to reveal the incriminating nature of an object, it could not have been seized in plain view).

364. Brenner & Frederiksen, *supra* note 108, at 96.

365. *See supra* Part II.B.2–3.

366. *Hicks*, 480 U.S. at 327.

367. Brenner & Frederiksen, *supra* note 108, at 70; *see also supra* notes 193, 219–21, 246–49 and accompanying text.

368. Brenner & Frederiksen, *supra* note 108, at 70–71.

369. U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 29 (1st ed. 2001).

370. *Id.* at 42.

Comprehensive Drug Testing.[371] This concern with limiting discretion waned over time, as the DOJ now directs its officers to "[a]void drafting warrants that would unnecessarily restrict the scope of the search."[372] Officers on the ground have taken the advice and assume a wide range of discretion, continuing aggressively and "undaunted" in viewing any file they deem necessary to "confirm" any suspicions they may have.[373] This is directly contradictory to the principle, established prior to the American Revolution, and essential to the Fourth Amendment and its jurisprudence : discretion should lie with the magistrate, and an officer should not be permitted to search wherever he sees fit.[374] Practical difficulties in limiting digital searches does not mean that these searches should not be limited.[375]

2. The Traditionalist Approach Seriously Threatens the Protection of Fourth Amendment Rights

The balancing approach employed by many courts in the past century has generally led to a dilution of Fourth Amendment principles.[376] Without close attention to the original principles underlying the Fourth Amendment, the governmental need to fight crime will almost always provide a compelling argument to outweigh the privacy of accused criminals.[377] 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.

Courts have made little progress in forming a workable doctrine on how best to protect against the dangers computer searches and the strict application of the plain view doctrine pose to the founding principles underlying the Fourth Amendment. The lax methods proposed by law enforcement and accepted by courts leave this vulnerable area of Fourth Amendment law open to interpretation and abuse. The suggestion by some courts and scholars that the law of reasonableness develop incrementally may not work.[378] Courts today are grappling with the same exact question they faced over a decade ago.[379] 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. Yet, courts continue to ignore these fundamental problems by applying the plain view doctrine to digital searches in the same manner as physical searches.

---

371. *Id.* at 43–44.
372. DIGITAL EVIDENCE IN THE COURTROOM, *supra* note 141, at 10.
373. *See supra* notes 220, 237, 258–60, 280–301 and accompanying text.
374. *See supra* notes 33, 48–57, 68–71, 93–95 and accompanying text.
375. *See* Michael, *supra* note 20, at 919.
376. *See supra* notes 72–78 and accompanying text.
377. *See* Michael, *supra* note 20, at 919.
378. *But see* United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010); Kerr, *supra* note 145, at 1277–78.
379. *Compare* United States v. Stabile, 2011 633 F.3d 219, 239–40 (3d Cir. 2011) (examining whether the plain view doctrine applies to file headers and file contents), *with* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (same).

The traditionalist approach of the Fourth and Seventh Circuits essentially permits any incriminating information found when searching each individual file on a given digital database to be used as evidence.[380] The Third Circuit, while advocating incremental progress in the development of reasonableness guidelines, only further encourages vague rules and the lax attitude of law enforcement discussed below by leaving this question open.[381] Over objections by appellants, traditionalist courts permit actions that they admittedly find troubling[382] while contrarily counseling caution and respect for privacy.[383] Setting aside the issue of inadvertency, while doctrinally correct, ignores the fundamental incongruity of the officers' actions in these cases when considering the Framers' intention to end such abusive practices. Attention to this intent would categorically deny allowing officers to "confirm" mere suspicion of crimes outside the scope of the warrant.[384]

As is evident from the sample cases outlined in Part III, courts are much less willing to bend old doctrines where the underlying crimes are more socially objectionable.[385] While "understandable abhorrence of [child pornography] can infect judicial judgment. . . . the Fourth Amendment do[es] not depend on the nature of the suspected criminal activity, any more than . . . on the race or gender of the suspect."[386] It ignores the animating principle of the Fourth Amendment to apply its direction selectively—the right to be free from arbitrary police discretion must be constantly afforded to all individuals.[387] The focus should not be on the harm done to the defendant by allowing evidence to be admitted, but to the harm to society created by an erosion of Fourth Amendment rights, "particularly . . . where the issue is the searching of personal computers, on which more and more extremely sensitive information is stored."[388]

The traditionalist approach permits officers to conduct dragnet searches, which the Framers aimed to prevent. In every case, the officers, either admittedly or by implication, were clearly rummaging for evidence not specifically listed in the warrant.[389] In *Comprehensive Drug Testing*, the investigating officers attempted to seek the broadest warrant and subpoenas possible and continuously sought broader authorization after having already been limited by magistrate judges. Beyond this, they "completely ignored"

380. *See supra* notes 203–04, 219–20 and accompanying text.
381. *See Stabile*, 633 F.3d 219, 238 (2011).
382. *See Mann*, 592 F.3d at 786.
383. *See* United States v. Williams, 592 F.3d 511, 523–24 (4th Cir. 2010).
384. *See Stabile*, 633 F.3d at 242.
385. *Compare Mann*, 592 F.3d at 780–81 (defendant videotaped female locker room and found in possession of child pornography), *and Williams*, 592 F.3d at 514–16 (defendant threatened schoolchildren with sexual assault and found in possession of child pornography), *with CDT II*, 579 F.3d 989, 993 (9th Cir. 2009) (involving medical records of individuals not being charged with a crime).
386. United States v. Krupa, 633 F.3d 1148, 1157 (9th Cir. 2011) (Berzon, J., dissenting).
387. *But see* Moshirnia, *supra* note 123, at 626–35 (advocating a "crime-based" approach for when the plain view doctrine should or should not apply in digital searches).
388. *Krupa*, 633 F.3d 1148, at 1157 (Berzon, J., dissenting).
389. *See supra* notes 197, 213, 224–31, 251–53, 272–93 and accompanying text.

the terms of the warrants they received.[390] The lower court judges in these cases expressed their shock at the tactics of the officers to seize data for which they did not have probable cause, asking, "[W]hat ever happened to the Fourth Amendment? Was it . . . repealed somehow?"[391]

Officers cannot be afforded the opportunity to plead sufficient facts to establish probable cause for a relatively minor crime, or against nominal individuals, in the hopes that they will uncover evidence they suspect to be on the same computer database involving different crimes or other defendants.[392] As seen by the Ninth Circuit, the traditional mode of analysis can be particularly unpalatable when dealing with private business or medical records compared with child pornographers, counterfeiters, and drug dealers. Indeed the business community, spurred by increasingly aggressive investigatory tactics by federal agents, is gravely concerned about the "potentially broad reach of the plain view doctrine as applied to searches of computers."[393] They suggest business actors fight back against overreaching officers, through such means as constant supervision of investigators by corporate counsel and instructing employees to take care to not answer any intrusive questions posed by law enforcement besides legitimate ones aimed at identifying seizable material.[394] The potential for dragnet searches of businesses' digital records is immense and troubling considering the hostile attitudes and distrust toward large companies in the wake of the financial crisis. Allegations of minor accounting irregularities by low level employees could be used as pretext for officers to search any file they want for evidence of crimes for which no probable cause has been established. While it may be practical to allow for broad authorization to seize and search electronic data, the potential for abuse created by such lenient standards will lead to overreaching by law enforcement.

The actions and attitudes expressed by officers in these sample cases may even have satisfied the Tenth Circuit's original "subjective" analysis. However, the incredibly fact-sensitive nature of such subjective analysis is unworkable as a doctrine for all cases.[395] While the Tenth Circuit recognized this and held that its cases more generally raised the particularity standard in digital warrants, it failed to require sufficient restrictions, impose search limitations in every case, or take further steps to make sure such limitations are followed.[396]

The Ninth Circuit's original en banc decision—which imposed a new set of mandatory guidelines—was much more responsive to the perils posed by traditionalist interpretation. All of these measures are necessary to ensure

390. *See supra* note 315 and accompanying text; *see also CDT III*, 621 F.3d 1162, 1177 (9th Cir. 2010).

391. *CDT III*, 621 F.3d at 1177.

392. *See supra* note 93.

393. William F. Johnson, Steven M. Witzel, & Lisa H. Bebchick, *Expect the Unexpected: Prepare in Advance for a Search Warrant on Business Premises*, N.Y. L.J., Feb. 24, 2011, at 2.

394. *Id.*

395. *See supra* notes 271–72 and accompanying text.

396. *See supra* notes 273–79 and accompanying text.

compliance with the Fourth Amendment's call for particularity and its underlying purpose of curbing governmental discretion: a change in the way we view the plain view doctrine in digital cases; particularized warrants with specific justifications and search methodologies; and sufficient distance between a "zealous officer[] . . . engaged in the often competitive enterprise of ferreting out crime"[397] and the temptation of mass amounts of potentially incriminating information.[398] Despite the court's retreat in its revised opinion, officers and courts should view these as best practices to be employed in all cases.

3. Ex Ante Limitations Are Neither Constitutionally Impermissible Nor Improper

The imposition of prophylactic rules is necessary, and should not be found to be constitutionally impermissible[399] nor as unprecedented and far-reaching as the government contends.[400] The cases presented by Professor Orin Kerr that could arguably indicate a limited role for magistrate judges are unique and limited in scope, and do not address search protocols that may govern the proper limits of a digital search within the boundaries of the Fourth Amendment.[401] In *Lo-Ji Sales*,[402] magistrate-imposed restrictions did not make the method impermissible it was that the magistrate could not be neutral and detached where he participated in the search.[403] While the Court in *Dalia*[404] found magistrate guidance on how a wiretap is to be installed unnecessary, it is not analogous to conditions on how a computer search should be executed. Limiting how the wiretap would be installed would not protect any recognizable Fourth Amendment interests like a search protocol or other prophylactic protections that effectively narrow a search would. The Court in *Dalia* mentions that nothing in the Fourth Amendment says a warrant "must" include an outline on how it will be executed,[405] yet this is far from foreclosing that possibility where it is necessary to protect against what otherwise inevitably becomes a general search.

All these cases seem to stand for the proposition that only certain requirements are necessary to satisfy particularity, and that extensive restrictions are unnecessary. But, these requirements that the defendants in these cases petitioned for did not address the particularity as to the place to be searched and things to be seized. Limiting how a computer may be searched is in fact limiting the "place to be searched" and "the things to be seized." The restriction of computer searches is within the constitutional

397. Johnson v. United States, 333 U.S. 10, 13–14 (1948).
398. *See infra* Part IV.B.
399. *See supra* notes 150–59 and accompanying text.
400. *See supra* notes 336–38 and accompanying text.
401. *See supra* note 16 and accompanying text.
402. Lo-Ji Sales v. New York, 442 U.S. 319 (1979).
403. *Id.* at 326–27.
404. Dalia v. United States, 441 U.S. 238 (1979).
405. *Id.* at 257.

powers of magistrate judges to narrow the warrant sufficiently such that it is not converted into a general one. The American Law Institute has contemplated a continuing oversight role for magistrate judges for the past thirty years,[406] and courts have done so since the seminal cases that led to the Fourth Amendment.[407] Search protocols can be very useful in many situations,[408] and the intrusive nature of computer searches may make limiting search protocols and other magistrate-imposed restrictions almost a necessity.[409]

Ex ante protocols should not be understood as a departure from what is already required in any warrant. Warrants must state with particularity the places to be searched and the things to be seized. However, in the case of computer searches, describing the "place to be searched" as an entire directory, hard drive, or other digital storage medium with an incredible amount of information does not sufficiently limit a search as a warrant for an entire home would. Removed are the physical constraints that limit the searches of those spaces, and added is the plethora of information and records simply not present in the physical context.[410] In *Andresen v. Maryland*,[411] the Supreme Court found that, even in the much less invasive case of intermingled hard copy documents, "judicial officials[] must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy."[412]

Magistrate judges have imposed limitations on how warrants may be executed, finding it within their constitutional mandate to do so. At least one judge has found that they are part of the particularity requirement, merely ensuring the search will be narrow.[413] Such limitations are not as unprecedented as the government's rehearing brief in *Comprehensive Drug Testing* suggests;[414] in fact, the Ninth Circuit simply affirmed the magistrates' already restrictive limitations placed on the warrants that the officers ignored.[415] When there is a considerable worry about sufficient particularity—as is nearly always present in computer search warrants—it is "constitutionally required to address those issues [at the warrant stage] in a way that avoids the later suppression of evidence."[416] A magistrate judge may condition the seizure of all digital storage devices belonging to a

406. AMERICAN LAW INSTITUTE, A MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE, § 220.5 (1975) (advocating for the continued involvement of magistrate judges to determine what procedures should be followed in segregating relevant evidence from innocuous materials).

407. *See supra* note 33 and accompanying text.

408. United States v. Cartier, 543 F.3d 442, 447–48 (8th Cir. 2008).

409. United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009).

410. *See supra* Part II.A.

411. 427 U.S. 463 (1976).

412. *Id.* at 482 n.11.

413. *In re* Search of: 3817 W. West End, 321 F. Supp. 2d 953, 957 (N.D. Ill. 2004).

414. *See* Brief for the United States, *supra* note 335; *supra* notes 281, 335–38 and accompanying text.

415. *See supra* notes 293–94 and accompanying text.

416. *In re* Search of: 3817 W. West End, 321 F. Supp. 2d at 956, 962.

certain person on the later submittal of a search protocol.[417] Prophylactic rules encourage "scrupulous adherence" to the particularity requirement that the Supreme Court found to be important in preventing general searches.[418] Understanding "unreasonable" as the Framers did should lead to the conclusion that warrants that are not sufficiently limited with particularity violate fundamental legal principles and thus are per se unreasonable.[419]

B. Ex Ante Restrictions to Protect Fourth Amendment Rights in Searches of Digital Data

The potential for abuse discussed above is best addressed by the Ninth Circuit's original en banc decision in *CDT II*. This decision provided a new scheme to replace the traditional application of the plain view exception and change the way computers are searched to protect Fourth Amendment interests. These rules should guide the judiciary and law enforcement in the future investigation of cases involving digital evidence. This section discusses the rules that are most essential to Fourth Amendment interests in digital search cases.

1. Applications for Computer Warrants Should Contain Case-Specific Justifications for the Method of Search and Segregation

Allowing for basic concerns common to all computer searches to justify increased intrusion in the form of seizure, copying, and off-site search limited only by continuously renewable deadlines is not a sufficient means to ensure that officers act within the constraints of the Fourth Amendment.[420] On-site search should be the default assumption, with an additional warrant attainable if it is not reasonable or possible to postulate initially as to the necessity of other methods.[421] Magistrate judges should also maintain control over the process by which evidence is returned to its owners, and ensure that all non-relevant equipment, information, or files that are seized (or copied) are returned as quickly as possible.[422]

2. The Plain View Exception Should Apply Only to Evidence Reasonably Related to the Evidence Sought in the Warrant

The Seventh Circuit stated that it would be "drastic" to abandon the plain view doctrine entirely in digital searches.[423] The Ninth Circuit found that officers should "waive reliance" on the doctrine altogether.[424] It may be correct that the full release of the doctrine in digital cases overcompensates

417. *Id.*
418. *See supra* note 102 and accompanying text (describing the discussion in *Horton* of the particularity requirement and its ability to prevent Fourth Amendment abuses).
419. *See supra* notes 50–51 and accompanying text.
420. *See supra* notes 367–72 and accompanying text.
421. Brenner & Frederiksen, *supra* note 108, at 102.
422. *Id.* at 103–04.
423. United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010).
424. *See supra* note 329 and accompanying text.

for the relative danger to Fourth Amendment rights. The type of evidence subject to plain view could be more appropriately limited to include what would otherwise be uncovered in an appropriately limited search in the physical context. For example, in the *Mann* case, it would not be practical to limit the search merely to evidence of voyeurism of young girls to the exclusion of any child pornography or erotica found on the defendant's hard drive.[425] They involve the same types of files, the same defendant, and substantially the same type of crime. Furthermore, it would be nonsensical to exclude evidence of multiple crimes contained in a single file where that evidence still concerns individuals under investigation; if a single file contained evidence of multiple crimes, there is no reasonable expectation of privacy to justify ignoring the evidence that is not specified in the warrant.[426] It is not necessary to abandon what was a practical doctrine. However, it should be severely limited to the situations just discussed—involving the same files, types of crimes, or defendants—because of the inherent differences that make strict application of the plain view doctrine inappropriate.[427]

3. Digital Warrants Should Contain a Search Protocol Designed to Uncover Only That Evidence Authorized To Be Seized in the Warrant

Limiting any on-site or off-site search by an appropriate search protocol is one of the most important measures to ensure that computer warrants are not converted into general warrants. However, the use of automated search techniques is more effective in the investigation of certain crimes against certain individuals or entities. While investigations of large organizations pose substantial difficulties because of the large number of computers, storage media, and shared directories that may need to be searched, such searches are mostly text-based, as they involve locating records of white-collar crime or large-scale drug organizations.[428] Such files are easier to search than audio or video content because they are much more susceptible to keyword searches. Especially in cases where files are less likely to be surreptitiously labeled, as in many cases with illicit items like drug records or child pornography, keyword searches can provide sufficient limitations. Yet most searches will need to be limited further by other means.

Other means of limitation can be accomplished by the use of forensic software such as "EnCase," and "hashes" as discussed previously.[429] Well-planned use of these techniques has the potential to limit the search to relevant data by the least intrusive means possible; however, this process could turn up a number of false positives.[430] This can be further limited by manually isolating the search to those files created or modified in certain

425. *See supra* notes 206–11 and accompanying text.
426. Brenner & Frederiksen, *supra* note 108, at 105.
427. *See supra* Part IV.A.1–2.
428. *See* Brenner & Frederiksen, *supra* note 108, at 99 & n.180.
429. *See supra* notes 169–73 and accompanying text.
430. Brenner & Frederiksen, *supra* note 108, at 61.

date ranges, controlled by certain individuals, or of certain file types.[431] These techniques for manually isolating files can also be helpful in the execution of searches, not only for text, but also for audio, images, and videos.[432] Hashes contained in FTK software, such as that used in *Mann*,[433] should be used when investigating crimes related to those for which the DOJ possesses "flagged" files.

Ex ante restrictions of search techniques and protocols do not necessarily have to predict the exact circumstances of the pending search. They can provide flexible guidance, such as predicating the opening of certain files upon certain conditions like probable cause being met. Magistrate judges are not without experience in determining what would be an appropriate search beforehand, even without information about the specific files to be found. Many of the same issues of probable cause, particularity, and reasonableness recur in all computer searches, as is evidenced by the form language used by officers in applying for such warrants.[434] Furthermore, if the protocols are found to be too restrictive based upon the situation presented when a special master reviews the materials as discussed below, an investigator can apply for a new warrant and testify to the reasonableness of his proposed actions.[435] This likely would not lead to unreasonable delay or inconvenience.

Limiting searches by such protocols is not comprehensive and often requires the second step of a physical search to find relevant information.[436] The automated searches are based on strings of text-based characters contained in the files, and often miss relevant data.[437] Depending on the software used, automated searches also fail to reach files that have been compressed, encrypted, or deleted, and thus require recovery.[438] The search techniques for other types of files are likely limited to searching the format alone, not the content of such files.[439] Thus, while limiting the intrusiveness of a computer search necessarily involves trying to limit its scope, there likely will need to be additional rummaging to even find the relevant information for the prosecution of the crime contained in the warrant. Thus, to protect against such discretion being afforded to the government, the next limitation is perhaps the most important to prevent Fourth Amendment violations in the computer search context.

---

431. *Id.* at 97, 100.
432. *See id.* at 97.
433. *See supra* notes 213–15 and accompanying text.
434. *See supra* notes 193, 219–21, 246–49, 444 and accompanying text.
435. *See In re* Search of: 3817 W. West End, 321 F. Supp. 2d 953, 961–62 (N.D. Ill. 2004) (discussing methods officers may follow when search protocol is too restrictive).
436. *See supra* notes 169–76 and accompanying text.
437. Brenner & Frederiksen, *supra* note 108, at 61–62.
438. *Id.* at 62.
439. *Id.*

4. Segregation of Data Should Be Performed By a Court-Appointed Special Master

The magistrate overseeing a warrant for computer searches should insist upon the appointment of a "special master" to conduct the search in a way that follows the protocols included in the warrant.[440] The magistrates in *CDT* imposed such a restriction, but the investigators ignored the requirement.[441] Delegating the authority to manually search individual files to a special master will prevent the impermissible grant of broad authorization to the government that allows it to conduct dragnet searches. Special masters should be neutral third parties, or if proper procedures can be developed to ensure independence they may also be officers specially trained in computer forensics not assigned to the case under question. Special masters should receive all seized or otherwise copied files before they are reviewed by anybody else. They can then use the techniques described above to segregate data that is within the scope of the warrant, while excluding non-relevant evidence unless it closely relates to the crime specified in the warrant or is contained in the same file as evidence that the warrant authorizes to be seized.

Courts have long recognized the constitutional value of having such neutral third parties, experts in a given field, segregate data where the specter of a general search looms.[442] Appointing a special master assures that any authority to view files potentially outside the scope of the warrant is granted to an official unconnected to the investigation and uninterested in "extend[ing] a general exploratory search from one object to another until something incriminating at last emerges."[443] This may be the only way to avoid the "advertent or inadvertent exploitation of the plain view doctrine when officers must search large quantities of computer files."[444]

CONCLUSION

Reasonableness should not turn on a necessary function of police power; to the Framers, unreasonable simply meant that which violates fundamental legal norms.[445] The fundamental legal norms that underlie the Fourth Amendment lead to the conclusion that "the people" should not be subject to unreasonable searches and seizures until courts finally determine what is reasonable and unreasonable. The principles of the Framers cannot be

---

440. *See id.* at 105.

441. *See supra* notes 305–09, 315 and accompanying text.

442. United States v. Wuagneux, 683 F.2d 1343, 1353 (11th Cir. 1982) (praising similar procedures as "an attempt by the 'responsible officials . . . to assure that [the search is] conducted in a manner that minimizes unwarranted intrusions upon privacy'" (quoting Andresen v. Maryland, 427 U.S. 463, 482 n. 11 (1976))); Forro Precision, Inc. v. IBM Corp., 673 F.2d 1045, 1053–54 (9th Cir. 1982) (approving of and advocating the use of lay experts to segregate documents with complex subject matter on-site).

443. Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971); *see supra* note 13 and accompanying text.

444. Brenner & Frederiksen, *supra* note 108, at 105.

445. *See supra* notes 50–51 and accompanying text.

abandoned because a sudden technological change cannot be reconciled with past, incrementally-built doctrines. The Supreme Court has aptly applied these founding principles to new technologies in the past,[446] and taken a proactive stance in preventing the grant of licenses to the government to conduct fishing expeditions.[447]

The exclusionary rule, created well after the Fourth Amendment, does not protect the trampling of rights that occur from the unconstitutional rummaging that occurs in almost every digital search. Ex ante restrictions protect Fourth Amendment rights of persons threatened with an intrusive search that involves general rummaging through their entire lives as catalogued in computer data, records, and files. The people are not free from unreasonable searches and seizures if we allow those searches in all cases to be subject only to lenient ex post review. Ex ante restrictions will protect individuals never charged with crimes—who would otherwise receive no benefit from ex post review—from having their files subjected to general searches.[448] Officers should be "acting within [the] constraints established by the Fourth Amendment," not simply subject to reprimand after they have acted without regard for its underlying principles.[449]

If a man's home is truly to remain his castle and officers continue to be required to work within the constraints of the Fourth Amendment, a man's computer must be treated as his castle as well. The abuses that led to the drafting of the Fourth Amendment have not been abated, they have merely been transformed.[450] General warrants exist today through the strict application of the plain view doctrine to digital searches. It is of the utmost importance that the principles underlying the Fourth Amendment are considered, and officers are restricted from conducting unreasonable digital searches through the use of ex ante restrictions.

446. *See supra* note 69 and accompanying text.
447. *See supra* note 93 and accompanying text.
448. Brenner & Frederiksen, *supra* note 108, at 100.
449. *Id.*
450. Michael, *supra* note 20, at 931.