Looking For Trouble: An Exploration of How to Regulate Digital Searches

I. INTRODUCTION

Imagine that the cybercrime division of a local police force receives a report of fraudulent credit card purchases, and after linking subpoenaed credit card records to a particular shipping address, officers obtain a warrant to search the computer of the resident for evidence of identity theft and fraud. During a preliminary search of the suspect's hard drive, the investigators discover a folder marked "preteen porno pix" filled entirely with picture and video files. Knowing that the evidence they are looking for is almost certainly contained within a text file, they have little reason to believe that opening this folder will benefit the identity theft investigation and they probably know that doing so will likely be beyond the scope of the warrant. For obvious reasons, however, the investigators have concerns about the folder. Should they be allowed to get a warrant to open the folder, and if so, should its contents be admissible evidence of a crime unrelated to fraud or identity theft?

According to some circuits the answer is yes. This scenario, which roughly parallels the fact pattern from the Third Circuit case *United States v. Stabile*, implicates the use of the plain view exception to the Fourth Amendment, which allows investigators to use any incriminating evidence that is in their plain view as they conduct an otherwise warranted search.[1] Although the apprehension of a criminal in possession of child pornography is universally desirable, many privacy advocates are uncomfortable with the use of this plain view doctrine in the context of digital searches.[2] For physical searches, the plain view doctrine has a proximity restraint, as evidence can only be in plain view if the investigating officer is nearby.[3] In the digital context, where the contents of an entire hard drive are effectively "nearby," this proximity restraint no longer exists—prompting one commentator to liken digital searches to "an officer walking into the foyer of a mansion and being able to see in plain view every person

1. United States v. Stabile, 633 F.3d 219, 224–25 (3d Cir. 2011).

2. *See, e.g.*, RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 59–61 (2007) (noting that application of the standard plain view doctrine to digital property searches threatens personal liberty).

3. Leonard Deutchman, *Do Computer Searches Distort the 'Plain View' Doctrine?*, LAW TECH. NEWS (May 14, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202458173965&Do_Computer_Searches_Distort_the_Plain_View_Doctrine__&slreturn=20130019173648.

and object in the entire structure."[4] In light of this potential expansion of what constitutes plain view, how private are our digital files?

The question of how to constrain the scope of digital searches is one that has split the circuit courts but has yet to be squarely addressed by the Supreme Court.[5] Some courts have largely circumvented the issue by declining to treat digital searches differently than physical searches.[6] Alternatively, the Ninth Circuit recommends that magistrate judges employ a comprehensive set of prophylactic measures designed to prevent investigators from overstepping their bounds.[7] This Note will analyze the relative strengths and weaknesses of each approach from both a theoretical and legal perspective. Ultimately, this Note reaches the conclusion that the court should prohibit the use of the plain view doctrine in the digital-search context, unless the original search is for evidence of a limited number of "flagged crimes"—sex crimes, crimes against children, or serious felonies.

This Note first explores the proposition that current methods for reviewing digital searches are insufficient to protect the privacy interests of suspects; it then evaluates various solutions to this perceived problem. Part II introduces the foundational doctrines that inform search procedure and outlines the unique characteristics of digital data that may make these doctrines inapposite to it. It then explores the circuit courts' different approaches to regulating digital searches. Part III weighs the strengths and weaknesses of several of these approaches, placing an emphasis on what measures are practical, efficient, accurate, and legally enforceable. Part IV suggests that courts should eliminate the plain view doctrine for all digital searches that are not investigating certain categories of crimes.

---

4. *Id.*

5. *Plain-View Doctrine Applies to Computer Searches, With Fact-Dependent Variations*, 16 Elec. Com. & L. Rep. (BNA) 268 (Feb. 23, 2011).

6. *See* United States v. Williams, 592 F.3d 511, 523–24 (4th Cir. 2010) (noting that the amount of information in a computer does not distinguish it from a file cabinet with a large number of documents).

7. *See* United States v. Comprehensive Drug Testing, Inc. (*CDT III*), 621 F.3d 1162, 1179–80 (9th Cir. 2010) (Kozinski, C.J., concurring) (listing the recommended guidelines for magistrate judges to consider when issuing digital-search warrants).

II. DIGITAL SEARCHES: WHAT IS THE PROBLEM AND WHY SHOULD I CARE?

While most Americans are probably aware of the importance of their computer files, very few are likely to have considered the implications of having those files searched by the government. This Part explores the constitutional basis for digital searches, the concerns that are unique to searching for digital files, and the different approaches that courts have taken to regulating digital searches.

A. The Fourth Amendment

The Fourth Amendment of the U.S. Constitution regulates government searches and seizures of property, and accordingly provides the foundational rules for digital searches. In relevant part, the Fourth Amendment states that "[t]he right of the people . . . 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."[8] Enacted to guard against the general warrants and writs of assistance that existed in England, this clause was intended to narrow the circumstances in which the government could conduct searches and to limit the techniques used in those searches.[9] To that end, it has retained a critical role, with the Supreme Court using the malleability of the word "reasonable" to balance the needs of law enforcement against the privacy interests of the people.[10] Reasonableness continues to be the "touchstone" of the Fourth Amendment,[11] and a full Fourth Amendment analysis is equally relevant in the digital-search context as it was to the physical-search context understood by the framers.

---

8. U.S. CONST. amend. IV.

9. Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 536 (2005).

10. *Id.*; *see also* Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1, 8 (2011) ("[T]he Court attempts to strike a straightforward 'balance between the public interest and the individual's right to personal security.' " (quoting Pennsylvania v. Mimms, 434 U.S. 106, 108–09 (1977))).

11. *See, e.g.*, Michigan v. Fisher, 130 S. Ct. 546, 548 (2009) (per curiam) (reiterating the Supreme Court's position that "the ultimate touchstone of the Fourth Amendment . . . is 'reasonableness' ").

B. The Plain View Doctrine

One of the greatest challenges of applying the Fourth Amendment to digital searches lies in determining how the plain view doctrine should operate in that context. The plain view doctrine is an exception to the usual Fourth Amendment requirements that allows investigating officers to use evidence discovered during a search, even though that evidence is unquestionably outside the scope of the warrant.[12] For the plain view doctrine to apply, several requirements must be met.[13] The Supreme Court listed these requirements in the 1990 case *Horton v. California*: (1) the officer cannot "violate the Fourth Amendment in arriving at the place from which the object could be plainly viewed," (2) "the object's incriminating character must be 'immediately apparent,' " and (3) "the officer must have a lawful right of access to the object itself."[14] Once these three requirements have been met, an officer can use any evidence he discovers—an unsettling prospect given the abundance of personal information that a digital search can bring into plain view.

C. The Unique Nature of Computer Data

Both the quantity and nature of data that is stored in digital formats make digital searches fundamentally different than physical searches. In many ways, this proposition is self-evident: opening a trash can, for example, is very different from opening a computer folder to view its files. As one commentator noted, some of these differences might have real implications for how officers approach investigations: "Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating

12. Chang, *supra* note 2, at 33.

13. If the use of the plain view doctrine were not limited to specific circumstances, there would be very little to functionally distinguish a particularized warrant from a general warrant. *See, e.g.*, Corey J. Mantei, *Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches*, 53 ARIZ. L. REV. 985, 991 (2011) ("[O]fficers may lawfully seize property located in open view if there is probable cause . . . . However, if these investigative efforts extend beyond the scope of a warrant . . . the government cannot utilize the plain view doctrine because this conduct constitutes a second, unauthorized search.").

14. Horton v. California, 496 U.S. 128, 128–29 (1990).

information."[15] Whether these differences merit the use of separate search regulations, however, is a controversial issue.

Perhaps the most obvious difference between digital files and physical files is that digital files require almost no physical space, which results in small objects (e.g., computers, flash drives, and cell phones) being filled with staggering amounts of data. Not only can computers now have hard drives with a terabyte of memory—enough to store one thousand copies of the Encyclopedia Brittanica[16]—but the number of people and households that currently have personal computers is enormous.[17] While some courts have rejected the notion that this difference in scale requires a new set of considerations,[18] others believe that it should shift the way in which the Fourth Amendment is applied, often insisting on additional restrictions designed to prevent searching through irrelevant files.[19] Obviously, the drafters of the Fourth Amendment did not contemplate searches of such unimaginably vast stores of information, so while their underlying concerns are certainly invoked, the applicability of the traditional Fourth Amendment framework is debatable.

Another salient characteristic of digital data is its intensely personal nature. This is especially true of data contained in personal computers. Indeed, the hard drive on most personal computers provides a remarkably complete profile of its user (or users). People actively save personal emails, pictures, videos, and even financial statements. Additional personal information such as instant messaging conversations may be stored automatically.[20] The total

---

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

16. Mantei, *supra* note 13, at 988 (citing *Megabytes, Gigabytes, Terabytes?... What Are They?*, WHAT'S A BYTE?, http://www.whatsabyte.com/ (last visited Oct. 18, 2012)).

17. *See* U.S. CENSUS BUREAU, HOUSEHOLDS WITH A COMPUTER AND INTERNET USE: 1984 TO 2009 (2009), *available at* http://www.census.gov/hhes/computer/index.html (finding that over 119 million U.S. households had personal computers in 2009).

18. *See, e.g.*, United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010) (concluding that the plain view doctrine rules for the search and seizure of non-electronic files should also govern electronic files).

19. *See, e.g.*, United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) ("[W]hen 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." (quoting United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999))).

20. Although instant messaging conversations are often saved remotely by the email client, and not necessarily on the user's hard drive, this information might still fall within the scope of a digital warrant, and is often saved automatically. *See, e.g.*, *Chat History*, GOOGLE SUPPORT,

collection of these files is likely to tell an investigator far more about the suspect than the search of any single physical space. Additionally, unlike physical spaces, in which owners presumably control what is kept and what is discarded, most hard drives do not eliminate data after an owner has "deleted" it, but only when it has been overwritten.[21] This makes it difficult for an average user to control the information stored on his or her hard drive, potentially giving rise to situations where investigators can search through deeply personal files that the suspect had intended to discard years earlier.

D. Circuit Court Approaches to Regulating Digital Searches

Probably because of the modern and evolving nature of digital searches, the Supreme Court has not yet ruled specifically on the applicability of the plain view doctrine to digital searches.[22] Given that Congress has also failed to address this issue directly, a variety of different approaches have emerged among federal district and state courts.[23] These different approaches touch on a broad range of issues that pertain to digital searches, including the degree of similarity between physical and digital searches,[24] what it means to be "in plain view" on a hard drive,[25] and whether the investigator's subjective intent should affect the application of the doctrine.[26] While it is presently unclear which, if any, of these issues will be addressed if the Supreme Court hears a digital-search case, the circuit courts are

---

http://support.google.com/chat/bin/answer.py?hl=en&answer=161925 (last visited Oct. 18, 2012) ("Chat history is enabled by default for Gmail users.").

21. *See e.g.*, Cynthia Senicka, *What Happens to a File When It's Deleted?*, IDAHO ST. U. HELPDESK, http://helpd.isu.edu/index.php?action=knowledgebase&catid=79&subcatid=82&docid=182 (last visited Oct. 19, 2012) ("The file does not go away at all when it is deleted. It only allows the space to be overwritten."); *see also* Chang, *supra* note 2, at 53 ("[C]ontained within every computer is a hidden trove of deleted files that many people believe are unrecoverable.").

22. *See Plain-View Doctrine Applies to Computer Searches, With Fact-Dependent Variations*, *supra* note 5 (noting that the Supreme Court has not considered this issue "which has been popping up in the lower federal courts and state courts for decades").

23. Mantei, *supra* note 13, at 992.

24. *See* United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010) (noting that the amount of information in a computer does not distinguish it from a file cabinet with a large number of documents).

25. *See* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (noting that while the full question of "what constitutes 'plain view' " in computer searches would not be reached by this court, image files that existed within closed files were not in plain view).

26. *See* United States v. Stabile, 633 F.3d 219, 240 (3d Cir. 2011) (finding that "an investigator's subjective intent is not relevant to whether a search falls within the scope of a search warrant").

currently divided into three primary camps: (1) those that apply the plain view doctrine as it applies to physical searches (the ex post–reasonableness-review approach), (2) those that apply the plain view doctrine only when the investigator inadvertently discovers evidence outside the scope of the warrant (the ex ante–limitation approach), and (3) those that recommend waiving reliance on the plain view doctrine in the context of digital searches (the plain view doctrine–abolishment approach).[27] Each of these approaches is explored in turn.

1. Applying the Plain View Doctrine Without Restriction: The First, Third, and Fourth Circuits

Although privacy advocates often argue for a more narrowly tailored set of Fourth Amendment requirements for digital searches,[28] others contend that the differences between digital and physical searches do not merit any separate considerations.[29] Implicit in this latter view is that the plain view doctrine should apply to digital searches as it does to physical searches. This approach has the advantage of being constitutionally uncontested, and it avoids the accusations of judicial overreaching that inevitably arise when courts promulgate their own regulations.[30] The First, Third, and Fourth Circuits, while all acknowledging the unique set of privacy concerns that might be implicated, have demonstrated a willingness to apply the traditional plain view doctrine to digital searches.

---

27. This recommendation was relegated to a concurrence, *CDT III*, 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, C.J., concurring), so it is a little misleading to characterize the Ninth Circuit this way. Because the recommendation still stands as guidance to magistrate judges, however, it is worthwhile for the purposes of this Note to explore its implications. *Id.* ("[It is] useful to provide guidance about how to deal with searches of electronically stored data in the future so that the public, the government and the courts of our circuit can be confident such [digital] searches and seizures are conducted lawfully.").

28. *See generally* Kerr, *supra* note 9 (exploring various ways in which the Fourth Amendment could apply to modern technology given basic differences between physical and digital searches).

29. *See Williams*, 592 F.3d at 523 (holding that a computer search is analogous to a file cabinet search); *see also* United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008) ("[N]either the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth Amendment context.").

30. *See, e.g.*, Allen H. Quist, Note, *Flexing Judicial Muscles: Did the Ninth Circuit Abandon Judicial Restraint in* United States v. Comprehensive Drug Testing, Inc.*?*, 24 BYU J. PUB. L. 371, 372 (2010) (arguing that the set of guidelines promulgated by the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.* were misguided and overbroad).

The First Circuit recently addressed this issue in *United States v. Farlow*.[31] In *Farlow,* the defendant sent sexually suggestive emails to a detective posing as a fourteen-year-old boy, resulting in a warrant to search the defendant's computer for evidence of "dissemination of indecent materials to minors or endangering the welfare of a child."[32] When the investigating detective searched the computer for images that allegedly had been sent by the defendant, he discovered child pornography and secured a second warrant for the search of that crime as well.[33] The defendant subsequently moved to suppress this evidence, claiming that the initial warrant did not describe the parameters of the search with enough particularity, as is required by the Fourth Amendment, and that the warrant would only have complied with this particularity requirement if it had mandated a specific type of search.[34] This motion was denied by both the magistrate and the district court.[35]

In holding that there was no obligation to mandate a particular search protocol, the court noted that "[w]ith the advent of the computer age, courts have struggled to balance privacy interests against law enforcement interests."[36] Nonetheless, it rejected the notion that the inclusion of a particular search protocol should be a warrant requirement.[37] Referring specifically to the search requirements suggested by the Ninth Circuit, which included abandoning the plain view doctrine, the court stated that these new requirements "create[d] more problems than [they] solve[d]," and that abandoning the plain view doctrine is "an extreme remedy better reserved for the unusual, not common case."[38] Instead, the court opined that the privacy interests implicated by digital searches would best be protected through case-by-case, fact-intensive inquiries into whether the warrant requirements were met and whether the investigator exceeded the parameters of the search warrant.[39] Referring to the First Circuit precedent established in *United States v.*

---

31. United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *4 (D. Maine Dec. 3, 2009).

32. *Id.* at *1.

33. *Id.* at *2.

34. *Id.*

35. *Id.* at *1.

36. *Id.* at *5.

37. *Id.* at *5–6.

38. *Id.* at *7 n.3.

39. *Id.* at *6.

Upham,[40] the court reaffirmed that a digital search was not inherently more invasive than a physical search and that the proper way to protect privacy interests was to require narrow and particular searches.[41] Accordingly, the *Farlow* court found that the plain view doctrine was applicable, without restrictions, to digital searches.[42]

Similarly, the Third Circuit held in *United States v. Stabile* that "the plain view doctrine applies to seizures of evidence during searches of computer files, but the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner."[43] In *Stabile,* a detective secured a warrant to search the defendant's hard drives for evidence of financial crimes, and subsequently encountered a folder of files containing names suggestive of child pornography.[44] Although the detective opened twelve of these files to "confirm" that they contained child pornography—likely expanding his search beyond the limits of the warrant—the court held that the lurid file names provided the probable cause necessary to justify a warrant for child pornography. Furthermore, because the court concluded that the investigation would have uncovered these files even if the detective had not expanded his search beyond the warrant, the doctrine of inevitable discovery prevented this misstep from invalidating the entire search.[45] The defendant challenged both the detective's decision to view the file names and the application of the plain view doctrine, but the court rejected both contentions and allowed the evidence to be admitted.[46]

Like the *Farlow* court, the *Stabile* court acknowledged society's competing interests in providing the government with sufficient leeway to conduct effective searches while still maintaining a requisite level of protection against general searches.[47] After reviewing the approaches from several other circuits, however, the *Stabile* court also declined to mandate a particular search protocol, electing instead to

40. United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) ("[A] search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for weapons or drugs.").

41. *Farlow*, 2009 WL 4728690, at *7.

42. *Id.*

43. United States v. Stabile, 633 F.3d 219, 240–41 (3d Cir. 2011).

44. *Id.* at 226–27.

45. *Id.* at 242, 246.

46. *Id.* at 237.

47. *Id.* ("On one hand . . . a broad, expansive search of the hard drive may be required. . . . On the other hand, as Stabile argues, granting the Government a *carte blanche* to search every file on the hard drive impermissibly transforms a 'limited search into a general one.' ").

focus on whether the search was focused and reasonable.[48] Within these general confines, the court found that the plain view doctrine was applicable,[49] noting that a "measured approach based on the facts of a particular case is especially warranted in the case of computer-related technology."[50] The determinative analysis, then, was whether the original plain view doctrine requirements of *Horton v. California*[51] had been satisfied.

It is the Fourth Circuit case *United States v. Williams*, however, that provided the most explicit support for treating digital and physical searches the same when it held that "the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents."[52] In *Williams,* a Baptist Temple received repeated emails referencing the author's intent to engage in sex acts with schoolboys, leading FBI agents to obtain a warrant to search the author's computers and digital storage media for "instrumentalities" indicative of the crimes of "Harassment by Computer."[53] When the agents eventually found thirty-nine images of child pornography on a DVD owned by the author, a second warrant was obtained, and the author was indicted for possession of child pornography.[54] The defendant's alternative contentions that the seizure of the DVD exceeded the scope of the warrant and that the plain view doctrine was not justified were both rejected by the court.[55]

Despite the defendant's argument that computer searches should be regulated using a framework of updated Fourth Amendment rules,[56] the *Williams* court used a traditional analysis, noting that this type of search "certainly counsels care and respect for privacy" but that it should not "undermine [the agent's] authority to search a computer's files."[57] Instead of using a different framework to address computer searches, the court focused on the reasonable limits of an

48. *See id.* at 238–40 (finding the detective's search to be reasonable in part because it was a "focused search of the hard drives rather than a general search").

49. *Id.* at 241.

50. *Id.* at 241 n.16 (quoting *CDT III*, 621 F.3d 1162, 1184 (9th Cir. 2010)).

51. *See* Horton v. California, 496 U.S. 128, 128–29 (1990) (citing Coolidge v. New Hampshire, 403 U.S. 443 (1971)) (listing requirements of the plain view doctrine).

52. United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010).

53. *Id.* at 515.

54. *Id.* at 516 n.2.

55. *Id.* at 514.

56. *Id.* at 517.

57. *Id.* at 523–24 (citing United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008)).

effective search and declined to put any limitations on the use of the plain view doctrine. In no uncertain terms, the Fourth Circuit rejected the notion that digital searches should be approached differently than physical searches: "We have applied these rules successfully in the context of warrants authorizing the search and seizure of non-electronic files . . . and we see no reason to depart from them in the context of electronic files."[58]

2. Adding an Inadvertence Requirement: The Tenth and Seventh Circuits

For those courts more focused on the potential invasiveness of digital searches, limiting the applicability of the plain view doctrine offers a means for protecting the privacy of defendants. Although the requirements of the plain view doctrine were well established in *Horton v. California,*[59] several courts have added an inadvertence element that requires the investigator to have inadvertently discovered any evidence in plain view that falls outside the warrant.[60] This element provides the obvious advantage of prohibiting an investigator from using a warrant pretextually to conduct a general search for a variety of crimes, and it offers a second defense against general searches after the particularity requirement of a warrant has been met. Even though this requirement is arguably in contravention of Supreme Court precedent, the Tenth Circuit and, perhaps, the Seventh Circuit[61] accept inadvertence to be a necessary precondition of the application of the plain view doctrine in digital searches.

The Tenth Circuit was the first circuit to directly address the applicability of the plain view doctrine to computer searches, in the 1999 case *United States v. Carey,*[62] and it limited the doctrine's applicability to those circumstances in which the investigator inadvertently discovered incriminating evidence of a crime not listed in the warrant.[63] In *Carey,* officers searched the defendant's computers

58. *Id.* at 524 (citing United States v. Crouch, 648 F.2d 932, 933–34 (4th Cir. 1981)).

59. Horton v. California, 496 U.S. 128, 141 (1990).

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

61. *See infra* note 80 (referring to the Seventh Circuit's determination that the plain view doctrine is unavailable when an investigating officer knew or should have known that files were outside the scope of a warrant).

62. Mantei, *supra* note 13, at 993.

63. *Carey*, 172 F.3d at 1273 n.4 ("Given the officer's testimony that he inadvertently discovered the *first* image . . . our holding is confined to the subsequent opening of numerous files the officer knew, or at least expected, would contain images [outside the scope of the warrant].").

for "evidence pertaining to the sale and distribution of controlled substances."[64] After discovering child pornography on a file the detective "was not familiar with," he proceeded to view the contents of nineteen disks before returning to his search for evidence of drug transactions.[65] Despite the detective's contention that he was not conducting a search for child pornography, the court suppressed the contents of these files, finding that he had "temporarily abandoned that [drug] search to look for more child pornography" and that the plain view doctrine was therefore inapplicable.[66]

Referencing the Supreme Court's decision in *Coolidge v. New Hampshire,* the *Carey* court reaffirmed that "the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at least emerges."[67] In *Carey*, the detective had suspicions that opening additional image files would uncover evidence of child pornography and not of drug crimes; therefore, the court held that these files were not uncovered accidentally but were purposely found during an unwarranted search.[68] In reaching this conclusion, the court focused on the fundamental differences between computer and physical searches, and determined the former should counsel toward a more restrictive set of search methods.[69] The court qualified the opinion by noting that the decision was predicated on these specific facts,[70] and with that caveat, it listed a series of search methods designed to prevent officers from conducting overbroad computer searches.[71]

In the 2009 case *United States v. Burgess*, the Tenth Circuit acknowledged the inadvertence requirement set forth in *Carey*, but emphasized that the search methods it proffered were fact specific and of limited applicability.[72] In *Burgess*, the investigating officer found images depicting child sexual exploitation while searching the

64. *Id.* at 1270.

65. *Id.* at 1271.

66. *Id.* at 1273.

67. *Id.* at 1272 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971)).

68. *Id.* at 1273.

69. *Id.* at 1274–75.

70. *Id.* at 1276.

71. *Id.* (citing Winick, *supra* note 15, at 107) (listing specific search methods like "observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory").

72. United States v. Burgess, 576 F.3d 1078, 1092 (10th Cir. 2009).

defendant's hard drive for evidence of drug trafficking.[73] Relying primarily on the precedent set in *Carey*, the defendant argued that the search violated the Fourth Amendment because it did not abide by the methods the *Carey* court outlined.[74] However, the court pointed out the factual differences between *Burgess* and *Carey*, noting that the agent in *Burgess* stopped his search and obtained a second warrant immediately upon discovering evidence of child pornography, thereby acting in accordance with the inadvertence requirement.[75] While leaving open the question of whether searches of digital files should be treated differently from those of physical containers,[76] the court emphasized that the search process must remain flexible enough to be effective in a variety of different circumstances.[77] As such, although the Tenth Circuit may have distanced itself from any search-method requirements, the inadvertence element of the plain view doctrine remains undisturbed in the digital-search context.

The Seventh Circuit, in the 2010 case *United States v. Mann*, provided a slightly different gloss on the inadvertence requirement when it indicated that the plain view doctrine is inapplicable to any evidence that the investigator knew or should have known was outside the scope of the warrant.[78] In *Mann,* detectives obtained a warrant to search the defendant's computer for evidence of voyeurism and used a forensic tool kit that highlighted any files that were known to contain illicit content (mostly child pornography).[79] When the detective opened four files that had been "flagged" in this manner, he discovered child pornography, but the court suppressed the files because the "flags" should have alerted the agent that they would be outside the scope of his warranted search.[80] Although the court noted that "intent is not generally relevant when assessing whether a given search falls within the scope of the warrant,"[81] it found that in this instance, the search

73. *Id.* at 1084 (noting that the investigating officer was searching for "trophy photos" of a person posing with stacks of money and drugs).

74. *Id.* at 1088.

75. *Id.* at 1092.

76. *Id.* at 1090 (referring to whether or not the search of a laptop computer should be subject to the same automobile exception as a briefcase). Given the facts of the case, the court did not have to reach this issue, noting only that the Supreme Court had not directly ruled on it. *Id.*

77. *Id.* at 1093.

78. United States v. Mann, 592 F.3d 779, 784 (7th Cir. 2010).

79. *Id.* at 781.

80. *Id.* at 784–85.

81. *Id.* (citing Platteville Area Apartment Ass'n v. City of Platteville, 179 F.3d 574, 580 (7th Cir. 1999)).

was unwarranted because the detective should have known better.[82] In the opinion of the Seventh Circuit, therefore, detectives should be prohibited from asserting that they inadvertently discovered evidence in plain view when they should have known it was outside the warrant; this rule supplements the original Fourth Amendment search requirements of reasonableness, particularity, and probable cause.

Notwithstanding its support in the Tenth and Seventh Circuits, an additional inadvertence requirement arguably contravenes Supreme Court precedent, and both the Fourth Circuit[83] and the Third Circuit[84] have rejected its legitimacy. Indeed, the Fourth Circuit noted that *Horton v. California* directly addressed the inadvertence issue and explicitly held that "it is not a necessary condition."[85] Similarly, the Fourth Circuit quoted the Supreme Court in *Maryland v. Garrison* for the proposition that a detective's subjective intent has no bearing on whether a search is within the parameters of a warrant.[86] Despite the requirement's laudable aim of providing additional privacy protections, the Supreme Court would likely need to qualify or overturn several prior holdings before inadvertence can be accepted as a necessary condition of the plain view doctrine.

3. The Ninth Circuit's Recommendation: Abandon the Plain View Doctrine

From an administrative standpoint, perhaps the cleanest solution to the concerns surrounding the use of the plain view doctrine in digital searches is to categorically prohibit it. Such a ban would provide a bright-line solution to the problem, ensure consistency across all courts and jurisdictions, and help to mitigate some of the privacy concerns that are attendant to digital searches. Although various courts have felt that abrogating the doctrine is an unnecessarily drastic response,[87] the Ninth Circuit proffered this

82. *Id.* at 784.

84. United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010).

84. United States v. Stabile, 633 F.3d 219, 240 (3d Cir. 2011).

85. *Williams*, 592 F.3d at 523 (quoting Horton v. California, 496 U.S. 128, 130 (1990)).

86. *Stabile*, 633 F.3d at 240 ("[T]he scope of a lawful search is defined by the object of the search and the places in which there is probable cause to believe it may be found." (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987))).

87. *See e.g.*, *Stabile*, 633 F.3d at 241 n.16 ("We decline to follow the Ninth Circuit's suggestion to 'forswear reliance on the plain view doctrine whenever the government seeks a

solution (among a variety of other measures designed to protect privacy in digital searches) in the heavily publicized 2009 case *United States v. Comprehensive Drug Testing, Inc.*[88] Although the majority opinion in that case was converted to a concurring opinion in a 2010 rehearing, it noted that "heeding this guidance will significantly increase the likelihood that the searches and seizures of electronic storage . . . will be deemed reasonable and lawful."[89] Accordingly, abandoning the use of the plain view doctrine for digital searches remains a viable solution for courts.

In light of the fact that the Supreme Court has not addressed the applicability of the plain view doctrine to digital searches, the Ninth Circuit's far-reaching and controversial approach significantly raised the stature of the issue.[90] In *Comprehensive Drug Testing* ("*CDT*"), the federal government investigated the Bay Area Lab Cooperative ("Balco") on suspicions that it had provided anabolic steroids to Major League Baseball players.[91] Having established probable cause for ten specific players, the government obtained warrants to search the facilities of CDT, an independent business that had conducted a series of anonymous and confidential drug tests for Major League Baseball, and the facilities of Quest Diagnostics, which stored the players' urine samples.[92] Despite clear notice that the warrants only granted access to the records of ten players, the government reviewed the testing records for hundreds.[93] Predictably, both CDT and the Major League Baseball Players Association moved to have the property returned—motions that were granted in both of the districts in which the respective companies were located.[94] After a

warrant to examine a computer hard drive.' "); United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010) (agreeing with the *CDT* dissent's position that abandoning the plain view doctrine is "overbroad"); United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *7 n.3 (D. Maine Dec. 3, 2009) ("[T]o require that the Government forswear the plain view doctrine is, in the Court's view, an extreme remedy better reserved for the unusual, not common case.").

88. United States v. Comprehensive Drug Testing, Inc. (*CDT II*), 579 F.3d 989 (9th Cir. 2009).

89. *CDT III*, 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, C.J., concurring).

90. *See Plain-View Doctrine Applies to Computer Searches, With Fact-Dependent Variations*, *supra* note 5, at 2–3 (explaining that other circuits have declined to follow the Ninth Circuit's approach).

91. *CDT II*, 579 F.3d at 993.

92. *Id.*

93. *Id.*

94. *Id.* at 994.

government appeal, an en banc panel in the Ninth Circuit upheld the decisions.[95]

Given the government's blatant disregard of its warrants, the Ninth Circuit's affirmation in *CDT* was not surprising, in and of itself. The court extended its opinion beyond this unremarkable holding, however, when it endeavored "to guide our district and magistrate judges in the proper administration of search warrants . . . for electronically stored information, so as to strike a proper balance between the government's legitimate interest in law enforcement and the people's right to privacy and property."[96] In this spirit, the court promulgated a set of prophylactic rules designed to safeguard against the type of brazen violations that the government had perpetrated. Specifically, Chief Judge Kozinski outlined five requirements for magistrate judges to meet when issuing a "warrant to examine a computer hard drive or electronic storage medium in searching for certain incriminating files,"[97] the first of which was that the government waive the use of the plain view doctrine.[98] By requiring the government to abandon the plain view doctrine, the court suggested that it would avoid the "illogical result" of allowing the particularity safeguards of warrants to be nullified.[99] "One phrase in the warrant cannot be read as eviscerating the other parts," wrote Chief Judge Kozinski, which would be the result if the government is allowed to keep "anything one of its agents happened to see while performing a forensic analysis of a hard drive."[100] By abandoning the plain view doctrine, therefore, the court was attempting to ensure that the boundaries of later search warrants would be respected, and that the plain view doctrine would not provide a loophole through which agents were able to evade the constitutional limitations of reasonable searches.

Chief Judge Kozinski's warrant requirements were binding law for only a brief period, however, since his opinion was relegated to a

---

95. *Id.* at 1007.

96. *Id.* at 994.

97. *Id.* at 1006 (citing United States v. Giberson, 527 F.3d 882 (9th Cir. 2008)).

98. *Id.* at 998. The remaining four requirements demand that the segregation and redaction of the property be done by an independent third party, that the warrant must disclose the actual risk of destruction of information, that the search be designed to uncover only the information for which the government has probable cause, and that the government must destroy or return any nonresponsive data. *Id.* at 1006.

99. *Id.*

100. *Id.*

concurrence when the court amended the *CDT* decision in 2010.[101] This revised opinion, while stripped of the authority of a majority opinion, still purported "to provide guidance about how to deal with searches of electronically stored data in the future," thereby creating a "safe harbor" that the government could rely upon in future searches.[102] Thus, while the prophylactic measures would no longer be *required* in the Ninth Circuit, scholars suggest that the use of these measures would create a strong presumption that the contested search would be permissible.[103] Because the obligatory nature of these measures had been such a dramatic departure from the status quo, this revision removed from the opinion its more contentious elements.[104] Nonetheless, these suggestions retain persuasive authority in the Ninth Circuit and represent an additional perspective on the applicability of the plain view doctrine in digital-search cases.

III. PROTECTING OUR PRIVACY: A CLOSER LOOK AT THE OPTIONS

In the words of law professor and renowned Fourth Amendment scholar Orin Kerr, "The widely-accepted goal of Fourth Amendment protection is to require reasonable police practices . . . [so] the question here is not what goal to achieve, but how to achieve it."[105] Clearly, there is considerable debate surrounding this question. Although the goal of ensuring reasonable search practices is uncontroversial, it is not clear that the police are failing to meet this goal. While there is a general consensus that digital searches provide a greater *potential* for unclear overreaching searches, there may not be an actual problem in practice. This is important to bear in mind, as limitations on government searches will inevitably allow some known

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

102. *Id.* at 1178 (Kozinski, C.J., concurring)

103. *See* Thomas J. Plumridge, Note, *The Fourth Amendment in a Digital World: Decoding* United States v. Comprehensive Drug Testing, Inc., 29 QUINNIPIAC L. REV. 197, 211 (2011) (referring to the measures "as something of a gold standard—not necessary in all cases as they were under *Comprehensive Drug Testing II*, but a solution that magistrates could employ to ensure that the Fourth Amendment is satisfied").

104. Orin Kerr, *Ninth Circuit Balks in BALCO Case, Denying Super En Banc in* United States v. Comprehensive Drug Testing *But Amending Opinion to Remove Challenged Section*, VOLOKH CONSPIRACY (Feb. 4, 2012, 12:52 PM), http://volokh.com/2010/09/13/ninth-circuit-balks-in-balco-case-denying-super-en-banc-in-united-states-v-comprehensive-drug-testing-but-amending-opinion-to-remove-challenged-section/ ("The truly dramatic and revolutionary parts of the original en banc *CDT* opinion are no longer Ninth Circuit law.").

105. Orin Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1247 (2010).

crimes to go unpunished—a legitimate societal problem in its own right. Given that the aversion to general warrants is so central to the Fourth Amendment, however, it might be necessary to preempt developments that may lead to unreasonable searches, irrespective of whether there is currently a problem.[106]

In light of this ambiguity, as well as the disagreements regarding whether digital searches should be considered separately in the first place, this Part evaluates the merit of the three general approaches that have emerged from the circuit courts: (1) applying ex post reasonableness review to searches; (2) placing ex ante limitations on searches; and (3) abandoning the use of the plain view doctrine. This Note suggests that the Court should abandon the use of the plain view doctrine for most digital searches, but should permit it for the investigation of several categories of crimes that are either related to child pornography or are particularly grave—sexual crimes, crimes against children, and serious felonies.

A. Applying Ex Post Reasonableness Review to Digital Searches: Applying the Plain View Doctrine Without Restriction

Performing ex post reasonableness reviews of digital searches, in the absence of any ex ante conditions or modifications of the plain view doctrine, is the traditional mechanism for ensuring reasonableness. Because there is no direct authority—statutory or otherwise—for the proposition that digital searches require separate treatment, reviewing these searches in the same manner as physical searches, if not required, is certainly not wrong.[107] Accordingly, this is probably the most prevalent approach of the three evaluated in this Part.[108]

Perhaps the greatest strength of ex post evaluations is that they allow for flexible, fact-intensive inquiries into how a particular

106. *See, e.g.*, Mantei, *supra* note 13, at 989 ("[T]he Framers wanted to prohibit the use of general warrants and writs of assistance, and thereby restrict the scope of government search authority." (citing Kerr, *supra* note 9, at 536)).

107. *See CDT II*, 579 F.3d 989, 1013 (9th Cir. 2009) (Callahan, J., concurring in part and dissenting in part) ("[T]he majority does not explain why it is now appropriate to grant heightened Fourth Amendment protections in the context of searches of computers based on the nature of the technology involved when we have previously cautioned just the opposite." (citing United States v. Giberson, 527 F.3d 882, 887–88 (9th Cir. 2008))).

108. Kerr, *supra* note 105, at 1280 ("Ex post review provides the standard method for developing the case law of the reasonableness of searches executed pursuant to warrants.").

search was conducted.[109] Given that the circumstances of different cases may necessitate significantly different search terms and methods, this approach allows judges to maintain oversight without requiring them to prescriptively dictate the terms of a digital search. Furthermore, because judges would be able to evaluate searches in light of the facts, there would generally be less error in judicial assessments of reasonableness than if reasonableness had been pursued through the use of ex ante conditions.[110] The advantages of evaluating searches on the facts of each specific case have often been cited as a reason to employ ex post review,[111] and these advantages are as appealing in the digital context as they are in the physical context.

In addition to providing more flexible and narrowly tailored analyses, ex post reviews of digital searches comport with the common law tradition of allowing the law (and the concept of reasonableness) to evolve over the course of numerous decisions. As opposed to ex ante conditions, which would be instituted broadly and at a single time, case-by-case analysis allows courts to "evaluate different cases over time to discern the most sensible rule given the technologies that develop."[112] This gradual and incremental approach can be expected to give rise to reasonableness requirements of the same sort as ex ante requirements, but with the advantage of having been built from the wisdom of numerous fact-intensive holdings.[113] This seems especially prudent given the unforeseen ways in which the relevant technology is

---

109. *See, e.g.*, United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *6 (D. Maine Dec. 3, 2009) ("[T]he far preferable approach is to examine the circumstances of each case, to assess the validity of the computer search protocol, to determine whether the police strayed from the authorized parameters of the search warrant, and to hold the police to constitutional standards in the context of a motion to suppress.").

110. Kerr, *supra* note 105, at 1281 (noting that "judges trying to impose ex ante restrictions generally will not know the facts needed to make an accurate judgment of reasonableness").

111. *See, e.g.*, United States v. Stabile, 633 F.3d 219, 240–41 (3d Cir. 2011) ("We hold that the plain view doctrine applies to seizures of evidence during searches of computer files, but the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner."); United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010) ("We are also skeptical of a rule requiring officers to always obtain pre-approval from a magistrate judge to use the electronic tools necessary to conduct searches tailored to uncovering evidence."); *CDT II*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part) (referring specifically to the abrogation of the plain view doctrine: "A measured approach based on the facts of a particular case is especially warranted in the case of computer-related technology"); *Farlow*, 2009 WL 4728690, at *6 ("[T]he far preferable approach is to examine the circumstances of each case.").

112. *CDT II*, 579 F.3d at 1018.

113. Kerr, *supra* note 105, at 1280 ("When repeated over time, this type of litigation leads to rules and standards governing the reasonableness of how warrants are executed.").

likely to develop over time.[114] Furthermore, several other areas of Fourth Amendment jurisprudence—including search-and-seizure law and the standard for valid stops—have evolved through fact-intensive, case-by-case developments, and it is not apparent why this application of the amendment should develop differently.[115] As such, ex post reasonableness reviews offer a variety of advantages that make it an attractive approach for courts evaluating digital searches.

The unfortunate flipside to the flexibility benefits offered by ex post reviews is the lack of clear standards and the resulting potential for inconsistent application among different courts. While a common law process might eventually bring the parameters of "reasonable digital searches" into focus, the vagueness of the standard in the meantime would almost certainly infringe on the privacy interests of some defendants. On the other hand, if investigators are unsure about the standards and rules that govern the reasonableness of their searches, they might conduct overly narrow searches in an attempt to avoid crossing the line, thereby limiting the investigative tools that are legally available to them.[116] In both cases, this inherent ambiguity obstructs the predictability needed to effectuate the protections of the Fourth Amendment.[117] Regardless of one's perspective on the proper balance between the interests of law enforcement and personal privacy, this uncertainty that accompanies ex post reviews could certainly be seen as an unacceptable drawback to their use.

B. Using Ex Ante Conditions to Limit Digital Searches

Imposing ex ante regulations to limit the scope of digital searches is an alternative, or possibly complementary, way for judges to restrict the outer limits of what is a constitutionally reasonable search. These sorts of regulations have found increasing use in recent

114. *CDT II*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part) ("A measured approach based on the facts of a particular case is especially warranted in the case of computer-related technology, which is constantly and quickly evolving.").

115. *See* Mantei, *supra* note 13, at 1001 (noting that "defining the requisite standard for valid stops (reasonable suspicion) and search-and-seizure law (probable cause)" occurred in this manner).

116. Chang, *supra* note 2, at 62–63 (noting that if courts were to review the reasonableness of specific forensic steps, the resulting confusion would likely result in police being more conservative in their searches).

117. *See* Bellin, *supra* note 10, at 26 ("Fourth Amendment doctrine must be sufficiently concrete that law-enforcement officers (and citizens) can predict, in advance, whether a given search or seizure is constitutional.").

years,[118] with the "high-water mark of judicial insistence on pre-approving search protocols" having been set in the *CDT* decision.[119] While there are a vast number of different regulations by which magistrate judges might seek to limit search methods, this analysis is limited to an evaluation of ex ante conditions as a general practice, the inadvertence requirement, and the search-protocol requirement.[120]

1. Ex Ante Warrant Regulations in General

The appeal of having magistrate judges regulate the terms of a digital search is nearly self-evident: instead of having to suppress the results of an unreasonable search *after* the government has rummaged through a suspect's property, ex ante regulations prevent invasive tactics altogether, thereby providing an added degree of privacy. Additionally, as the *CDT* court suggested in Judge Kozinski's opinion, magistrate judges "are in the front line of preserving the constitutional freedoms of our citizens while assisting the government in its legitimate efforts to prosecute criminal activity."[121] Since these judges are in a unique position to assess the circumstances surrounding each case, it seems sensible to defer to their judgment on how a particular search should be conducted. From both a constitutional and a normative standpoint, however, ex ante regulations are arguably defective and should be considered with some skepticism.[122]

The role of the judge in issuing a search warrant is described generally by the Fourth Amendment and more specifically by either federal or state statute.[123] None of these sources refer to an inherent authority for judges to dictate the terms or methodologies of a search. Instead, in applying the Fourth Amendment, a magistrate judge

---

118. *See* Kerr, *supra* note 105, at 1244 (noting the increased use and variety of ex ante limitations on warrants employed by courts).

119. *Id.* at 1256.

120. Professor Kerr has highlighted four primary kinds of limitations. This Note does not evaluate any restrictions that pertain to the physical search component of computer search and seizure, opting instead to analyze several specific conditions that are prominent among circuit courts. *See* Kerr, *supra* note 105, at 1244 (listing the four kinds of limitations).

121. *CDT II*, 579 F.3d 989, 1007 (9th Cir. 2009).

122. *See generally* Kerr, *supra* note 105 (arguing that ex ante regulations of searches are without constitutional or statutory authority, and that they are imprudent from a policy perspective as well).

123. *See id.* at 1271 ("Whereas the Fourth Amendment provides a general framework, warrant statutes explain the procedural details of who can obtain the warrant, how it can be obtained, when it can be executed, and how a return on the warrant must be filed.").

assesses probable cause, particularity, and any additional requirements derived from state or federal statute.[124] A series of Supreme Court opinions addressing various aspects of ex ante regulation[125] have established that magistrates are not permitted to play an additional role in the execution of search warrants,[126] that two-stage warrants[127] (as computer searches require) do not justify a separate set of rules,[128] that reasonableness limitations are prohibited,[129] and that ex ante regulations on searches do not have any legally binding effect.[130] Additionally, because most warrant laws require that an issuing judge "must" issue warrants once probable cause and particularity have been established, there is no statutory basis for magistrate judges to issue discretionary limitations on searches.[131] Accordingly, even though the Court has not explicitly invalidated ex ante regulations, there are a variety of indications that they might be invalid.

Assuming for the purposes of this analysis that ex ante conditions are of uncontested validity, their use is perhaps equally problematic from a normative standpoint.[132] While ex ante conditions do provide the advantage of prescriptively outlining the contours of a reasonable search—an idea explored in the following section—these conditions may introduce significant potential for error, thereby doing

---

124. *Id.* at 1261.

125. *See id.* at 1270–71 (summarizing the impact of four Supreme Court cases that combine to compel the conclusion that reasonableness must be assessed ex post).

126. *See* Lo-Ji Sales v. New York, 442 U.S. 319, 328 (1979) (invalidating the magistrate's decision to "telescope the processes of the application for a warrant, the issuance of the warrant, and its execution").

127. The first stage is the physical search stage, where the government retrieves the computer. The second stage is the digital-search stage, where the digital data is searched. *See* Kerr, *supra* note 105, at 1248.

128. *See* Dalia v. United States, 441 U.S. 238, 258 (1979) ("It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers.").

129. *See* United States v. Grubbs, 547 U.S. 90, 98 (2006) ("The language of the Fourth Amendment is likewise decisive here; its particularity requirement does not include the conditions precedent to execution of the warrant.").

130. *See* Richards v. Wisconsin, 520 U.S. 385, 395 (1997) (holding that the officers' blatant violation of the magistrate judge's "knock and announce" condition was not unreasonable, as the reasonableness of the decision "must be evaluated as of the time they entered" and not at the time the magistrate issued the warrant.).

131. Kerr, *supra* note 105, at 1261 ("The federal search warrant statute and most analogous state statutes use language that denies judges the power to reject warrant applications based on how they are executed.").

132. *Id.*

a disservice to the reasonableness goal that they are purported to serve.[133] In addition, ex ante regulations must be considered alongside ex post reasonableness reviews, which are the traditional methods of protection against Fourth Amendment violations.[134] As Professor Kerr has noted, this is not of much concern when the ex ante conditions are equally or less exacting than the ex post review requires.[135] However, when the ex ante conditions create limitations beyond what is required ex post, these conditions are erroneous by definition,[136] and they unreasonably impede the government's ability to investigate crimes.[137] Furthermore, as several commentators have noted in the wake of the *CDT* decisions, ex ante regulations are often resource intensive and difficult to administrate.[138] As a potentially difficult and expensive tool that often misses the mark of ensuring reasonable searches, the putative benefits of ex ante regulations may not be worth the questions and problems that they present.

2. The Inadvertence Requirement of the Plain View Doctrine

Although courts that add an inadvertence requirement to the plain view doctrine do not generally do so through ex ante regulations,[139] the practice involves an additional judicial constraint on how an investigator can approach a search. Accordingly, there is no analytical distinction between a magistrate judge adding this requirement as an ex ante condition and an appellate judge adding the requirement in a reasonableness review. It is important to note, however, that even if ex ante conditions are categorically illegitimate as per Section II.B.1 above, the inadvertence requirement could still be instituted in ex post hearings, and accordingly, this requirement

133. *Id.* at 1281.

134. *Id.* at 1280.

135. *Id.*

136. *Id.*

137. *Id.*

138. *See, e.g.*, Leonard Deutchman, *To Avoid 'Plain View,' Investigators Need Blinders*, LAW TECH. NEWS (May 19, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202458410399&To_Avoid_Plain_View_Investigators_Need_Blinders___ (noting, in response to several *CDT* conditions, that it would be expensive and difficult to find and train several sets of investigators, and "absurd" to assume that a set of independent analysts could perform their duties without discussing facts with case agents); *see also* Mantei, *supra* note 13, at 1000 ("The requirement of independent filter teams also creates logistical nightmares for both law enforcement agents and prosecutors.").

139. Indeed, the circuits that have acknowledged the inadvertence requirement have done so in ex post hearings, not through the issuance of ex ante conditions.

should be evaluated on its own merits. Because this restriction has been explicitly endorsed by the Tenth Circuit[140] and at least acknowledged by the Seventh Circuit,[141] it deserves analysis as a plausible method for restricting the scope of digital searches.

The overarching benefit of adding an inadvertence requirement to the plain view doctrine is that it prohibits *purely* pretextual searches.[142] This means, for example, that an investigator would be barred from using the guise of searching for tax fraud to deliberately search for evidence of identity theft. In theory, this requirement helps mitigate the underlying concern that the plain view doctrine can transform a particularized search warrant into a general search warrant, as investigators would be prohibited from searching for evidence of additional crimes, even if the methods of that search technically fall within the scope of the warrant.[143] Given that the purpose of the Fourth Amendment is to prevent the government from conducting general searches, this is certainly a salutary result, to the extent that it is realized.[144]

While the goal of ensuring more particularized searches is a good one, the inadvertence requirement does little to achieve it. First, there are few scenarios in which this requirement provides any additional protections. Presumably, if an investigator's search comports with the requirements of a warrant, then it would only violate the inadvertence requirement if it were clear that the investigator's intent was to find evidence of a crime not listed in the warrant. This intent would be difficult to establish both because most investigators would be unlikely to admit that they were deliberately flouting the warrant and because any search that comports with the terms of a search warrant (which has necessarily met the particularity

140. United States v. Burgess, 576 F.3d 1078, 1092 (10th Cir. 2009) (approving of the fact that the officer inadvertently found the first image of child pornography, then stopped the search and obtained a second warrant); United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).

141. United States v. Mann, 592 F.3d 779, 784 (7th Cir. 2010).

142. I emphasize the word "purely" to point out that while the inadvertence requirement prohibits an investigator from pretextually "searching" for evidence of a crime in which he is not interested, it is not clear that the inadvertence requirement prohibits that investigator from conducting a search in which he has at least *some* interest in the crime for which he has obtained a warrant.

143. *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971) ("[T]he 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.").

144. *See, e.g.*, Mantei, *supra* note 13, at 989 ("After breaking away from English rule, the Framers wanted to prohibit the use of general warrants and writs of assistance, and thereby restrict the scope of government search authority.").

condition) is almost certainly reasonable.[145] Given that an investigator is otherwise prevented from conducting searches outside the scope of the warrant, the inadvertence requirement would only apply when (1) the investigator admits that he was deliberately searching for evidence of a crime not within the warrant, or (2) the circumstances of the search directly demonstrate that the investigator was no longer searching for evidence of the crime within the warrant. Although one can envision cases in which either of these scenarios might unfold,[146] the cases in which the inadvertence requirement will make a difference in nullifying the plain view doctrine are likely to be rare.

In addition, adding an inadvertence requirement to the plain view doctrine would arguably require the Supreme Court to overturn precedent and would bring considerable change to the Court's Fourth Amendment jurisprudence.[147] Although the Court could make such a decision, the principle of *stare decisis* makes such a move unlikely in the context of constitutional interpretation. Especially in light of the nominal protections that the inadvertence requirement provides against invasive searches, it is unlikely to gain any significant traction in the Supreme Court.

3. Regulations Prescribing Particular Search Protocols

In an ideal world, the danger of overbroad searches and the privacy concerns that they implicate would be eliminated by a perfect search tool that provides the government with all the information responsive to its search warrant but nothing else.[148] Needless to say, this tool does not exist at present, and given the incentives for cybercriminals to develop countertechnologies, it may never exist.[149]

---

145. *See id.* at 996 ("[P]articularity renders any additional requirement for inadvertence unnecessary because any evidence seized outside the warrant's specific terms will be deemed inadmissible.").

146. The investigator's search through obviously pornographic files in *United States v. Carey* is an example of objective evidence of the investigator's intent to look for something other than the crime listed in the warrant.

147. *See e.g.*, Horton v. California, 496 U.S. 128, 130 (1990) (holding that inadvertence is not a "necessary condition" of plain-view evidence seizures); Maryland v. Garrison, 480 U.S. 79, 84 (1987) (determining validity of a search that inadvertently exceeded the warrant by imposing a reasonability test on the officer's actions).

148. *See* Kerr, *supra* note 9, at 570 (describing "Perfect Tool," which allows an investigator to "enter in the terms described in the warrant, and the tool will find that evidence and nothing else").

149. *See id.* ("Investigators and sophisticated wrongdoers inevitably play a cat-and-mouse game in which suspects try to hide evidence and forensic analysts try to find it.").

Despite this shortcoming, some courts have purported to mandate particular search protocols as a means for limiting the scope of digital searches.[150] Although warrants have historically met the particularity requirement when the search is limited to evidence of a specific crime,[151] warrants that limit searches to a *particular methodology* would almost certainly result in more focused, narrow searches. The relative merits of these mandated protocols are consequently worth a closer look.

Of all the ways in which courts might attempt to limit the scope of digital searches, ex ante regulations that prescribe particular search protocols are likely to be the clearest and most enforceable options. Search protocols offer bright-line rules that define reasonable behavior, and they are both easy for courts to administer and for investigators to follow. Because ex ante rules prevent investigators from employing methodologies that are not explicitly authorized, they can curtail the very *act* of general government searches, not just the government's subsequent use of evidence discovered through general searches.[152] It is this capacity to *prevent* certain government behavior, a feature that both ex post reasonableness reviews and the inadvertence requirement[153] lack, that enables search protocols to provide privacy protections that the other solutions cannot.

This ability to bind the conduct of investigators, however, is also the biggest weakness of regulating by search protocols. As the Tenth Circuit opined in *Burgess*, the search process must remain dynamic, and search protocol regulations would necessarily strip investigators of their ability to tailor and craft searches to the needs of

150. *See, e.g.*, *CDT II*, 579 F.3d 989, 1006 (9th Cir. 2009) (summarizing five points of guidance to prevent over-seizing evidence in a search)*; see also* United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) ("[L]aw enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing file types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory.").

151. *See* Chang, *supra* note 2, at 42 ("Generally, courts will find particularity if a crime is associated, however, loosely, with the evidence described in a warrant.").

152. Obviously, the fact that evidence can be suppressed if the search that uncovered it was unreasonable is of small consolation to a suspect who was primarily concerned with having various pieces of her property searched in the first place.

153. When issued ex ante, the inadvertence requirement would allegedly prevent investigators from engaging in certain types of behavior (e.g., deliberately searching for evidence of a crime not listed in the warrant). Because the limitation is defined by the intent of the investigator, however, and not the type of behavior itself, an ex ante inadvertence requirement would almost certainly be a less effective preventative restraint than would ex ante protocol requirements.

a particular case.[154] The restrictive nature of these regulations seems particularly draconian when one considers the potential impact that prescribed search protocols might have on how criminals create and store evidence of their crimes. For example, if judges were known to prohibit the review of any image files for evidence of identity theft, criminals might simply take photographs of these files, so as to store them in a format that they knew to be inaccessible to the government.[155] Intuitively, incriminating computer files are often mislabeled, and if there are specific restrictions regarding how investigators can search for those files, they are likely to be mislabeled in a way that allows them to avoid detection.[156] As the *Burgess* court concluded, "[I]t is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives."[157]

In addition to potentially crippling the government's ability to conduct effective searches, announcing ex ante conditions through search protocols would require judges to involve themselves in a technology-intensive arena that extends beyond their competencies.[158] This difficulty is compounded by the reality that each case raises a unique array of considerations, all of which the judge will need to understand before he is able to proffer a well-tailored set of search conditions. Thus, not only do ex ante conditions demand that magistrate judges familiarize themselves with the details of the case from the earliest proceedings, but they also require that judges have the technical sophistication to employ those facts to craft a search strategy that narrowly, but effectively, enables investigators to find evidence responsive to the warrant. As the *Farlow* court surmised,

---

154. United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009) ("It is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods.").

155. Corey Mantei suggests a slightly different scenario in which criminals might mislabel evidence of one crime to indicate a different form of illegal activity, knowing that investigators would be prohibited from inspecting any files that suggest evidence of a crime outside of the warrant. Mantei, *supra* note 13, at 1009.

156. *See, e.g.*, United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) (justifying broader searches based on the described categories of the warrant, saying, "[T]he reality [is] that few people keep documents of their criminal transactions in a folder marked 'drug records' "); *see also Burgess*, 576 F.3d at 1093 ("The directory structure might give hints as to an effective search strategy, but could just as well be misleading and most often could not effectively, or even reasonably, be described or limited in a warrant.").

157. *Burgess*, 576 F.3d at 1094.

158. *See* United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *7 n.3 (D. Maine Dec. 3, 2009) (referring to the challenges that search protocols present to issuing judges).

"Even the most computer literate of judges would struggle to know what protocol is appropriate in any individual case . . . ."[159] Accordingly, courts should be hesitant to impose on them a task for which they are so ill suited.

C. Abandoning the Plain View Doctrine Altogether

Arguably the most contentious method for restraining digital searches is to require that investigators abandon the use of the plain view doctrine, thereby restricting the admissible evidence to only that which specifically falls within the four corners of the warrant. This method can be effectuated either by requiring that investigators agree to waive the use of the doctrine or by enlisting independent third parties to separate the seizable from the nonseizable data.[160] In either scenario, investigators are unable to use anything other than evidence of the listed crime. Although there is no basis in Supreme Court precedent for abandoning this doctrine,[161] the profound potential it has for limiting digital searches has enabled this approach to gain favor among several scholars and commentators.[162] It is accordingly worth exploring this option in more detail.

Defendants reap a variety of benefits when the government is unable to use the plain view doctrine, most of which stem from the significant restrictions on the evidence that can be used against them. Although this solution does not *prevent* investigators from conducting broad searches in the same way that prescriptions for search protocols would, the fact that any outside evidence would be inadmissible is

159. *Id.*

160. *CDT II*, 579 F.3d 989, 998 (9th Cir. 2009) ("[T]he government should . . . forswear reliance on the plain view doctrine . . . . If the government doesn't consent to such a waiver, the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether.").

161. *See id.* at 1017 (Bea, J., concurring in part and dissenting in part) ("Such a rule departs from existing Supreme Court precedent regarding the 'plain view' exception to the Fourth Amendment's warrant requirement, and do[es] so without a single citation to the Supreme Court's extensive precedent on the subject.").

162. *See generally* Chang, *supra* note 2, at 65 (arguing that the plain view doctrine should not be used in the digital-search context); Kerr, *supra* note 9, at 583 (arguing that it is premature for courts to drop the doctrine, but that "[i]n time, abolishing the plain view exception may best balance the competing needs of privacy and law enforcement in light of developments in computer technology and the digital forensics process").

likely to reduce investigators' incentives to conduct broad searches.[163] In addition, since the plain view doctrine is often alleged to allow investigators to treat a digital-search warrant like a general warrant, abolishing its use contributes in a meaningful way to the realization of Fourth Amendment goals.[164] It is also important to note that this solution does not implicate either the independent source rule or the inevitable discovery rule, which allow the government to use evidence that would have been discovered via alternative methods.[165] Thus, these rules "can ensure that the police are not placed in a worse situation by finding evidence pursuant to a broad search, but that neither are they in a better position."[166] Abolishing the plain view doctrine for digital searches, therefore, can eliminate some objectionable aspects of these searches, while still retaining tools needed for law enforcement to remain effective. As such, this may be a realistic way to align workable government protocols with the privacy expectations of the general public.[167]

The most common criticism of this abolishment theory is that it is overbroad and would eventually lead to undesirable results. The *Farlow* court, in a lengthy footnote, provided a particularly unnerving hypothetical example of how this might play out:

> In a future case, the evidence in plain view could be profoundly serious, ranging from photographs of a kidnapped child to plans to commit acts of terrorism. The judicial directive to forswear in advance the plain view doctrine, placed in a different context, is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair.[168]

Clearly, this is a disturbing example designed to repulse the reader, but the court's point is well taken—abolishing the plain view doctrine

---

163. *See* Kerr, s*upra* note 9, at 584 ("In short, it would allow the police to conduct whatever search they needed to conduct (to ensure recovery) and then limit use of the evidence found (to deter abuses).").

164. *See* United States v. Williams, 592 F.3d 511, 518 (4th Cir. 2010) (noting that the defendant had asserted that "[t]o apply the plain-view exception in the context of computer searches would . . . 'effectively read [ ] the warrant requirement out of the Fourth Amendment.' "). *But see* Deutchman, *supra* note 138, at 5 (noting that several courts have not found that the plain view doctrine is inconsistent with the Fourth Amendment: "The other circuits that have taken issue with the 9th Circuit have done so because they have not seen law enforcement using the plain view exception to subvert the Fourth Amendment").

165. *See* Kerr, *supra* note 9, at 584.

166. *Id.*

167. *See* Chang, *supra* note 2, at 65 (contending that the elimination of the plain view doctrine would create "the added benefit that the law would be more in line with society's expectations").

168. United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *7 n.3 (D. Maine Dec. 3, 2009).

is a broad solution with very few exceptions,[169] and its lack of flexibility could potentially lead to unconscionable results. Even commentators who believe that this may eventually be the best way to rein in digital searches have been hesitant to employ such a drastic measure at present,[170] and the bulk of courts that have considered this solution have opted instead for a more "considered" approach that allows the plain view doctrine to develop incrementally.[171] When combined with the fact that there is no precedent for its abolishment,[172] the severity of abandoning the plain view doctrine is troublesome.

A strong indicator that the abolishment solution is overbroad is the fact that in *CDT*—the very case in which this solution was originally promulgated—there were narrower restrictions that would have addressed the government's transgressions. Without question, the government's searches through the records of players who were never listed in the warrant were patently unreasonable from an ex post perspective. Similarly, those searches would not have been admissible if an inadvertence standard were used, and there is no conceivable set of mandatory search protocols that would have permitted the government to expand its search methods to reach so far beyond the records of suspected players. Because the government's behavior in *CDT* could have been remedied by several more specific solutions, the comparatively drastic measure of abolishing the plain view doctrine for all digital searches seems to have been unnecessary.[173]

Bearing in mind the Ninth Circuit's laudable goal of providing clarity to the process of issuing digital search warrants, promulgating

---

169. Presumably, the independent source and inevitable discovery exceptions would still apply.

170. *See* Kerr, *supra* note 9, at 583 ("The need for new rules is emerging, but eliminating the plain view exception would be too severe at present.").

171. *See, e.g.*, United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010) ("We too believe 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.' " (quoting *CDT II*, 579 F.3d 989, 1013 (9th Cir. 2009) (Callahan, J., concurring in part and dissenting in part))); *see also* United States v. Stabile, 633 F.3d 219, 241 (3d Cir. 2011) (agreeing with the Seventh Circuit in *Mann*, that the plain view doctrine should be developed incrementally).

172. *CDT II*, 579 F.3d at 1017 (Bea, J., concurring in part and dissenting in part).

173. *See* Deutchman, *supra* note 138, at 4 ("[S]anctions specific to the facts in Comprehensive Drug Testing could have been imposed without imposing the 9th Circuit's protocol for all computer search cases."); *see also CDT II*, 579 F.3d at 1012 (Callahan, J., concurring in part and dissenting in part) ("The majority's prescriptions go significantly beyond what is necessary for it to resolve this case.").

overbroad search restrictions is imprudent because it will necessarily strip the government of its ability to prosecute known offenders.[174] This is especially troubling when one considers the frequency with which these cases involve child pornography: an especially repugnant crime.[175] Furthermore, the technology that enables digital searches is sure to develop in the years to come, which is likely to change the landscape of how investigators can search and what evidence is brought to their attention. Given this flux, categorically dismissing the plain view doctrine seems both drastic and shortsighted.[176]

IV. A SOLUTION THAT FITS THE CRIME

Clearly, the question of how to address the privacy concerns that arise during the course of a digital search is a complicated one. In theory, the ideal solution would address the concerns that are unique to the digital context without impeding the government's investigative duties.[177] In practice, however, this is a difficult balance to strike, and the appropriate resolution of the problem likely depends on whether one's sympathies lie more with personal privacy interests or with the law enforcement interests of the state.[178] Fully acknowledging that each of these interests is critically important to a free and functioning society, this Note suggests a novel solution that has not been tried by

---

174. *See* Chang, *supra* note 2, at 66 (noting that as a result of eliminating the plain view doctrine, "Society may suffer from unintended consequences such as unpunished criminal conduct. Thus far, most digital property plain view cases seem to involve child pornography and, of course, there is nobody who wants criminal pedophiles to escape justice.").

175. *See id.* at 61 (explaining that "child pornography is the crime that has been implicated in most of the reported cases dealing with the application of the plain view doctrine to digital evidence").

176. *See* Mantei, *supra* note 13, at 1011 ("By eliminating the plain view doctrine's application in computer searches, courts would be unnecessarily handicapping government search efforts. As computer technology continues to improve, less invasive search tools may become common in all jurisdictions. . . . It is almost impossible to predict the future of search-and-seizure technology.").

177. *See* Kerr, *supra* note 9, at 536 (noting that the term "reasonable" has "permitted the Supreme Court to craft a set of rules that balances law enforcement needs with individual interests in the deterrence of abusive law enforcement practices.").

178. For most people, one's sympathies fall somewhere along a spectrum that appreciates the interests of both parties. *See id.* at 536 n.11 ("Innocent suspects would presumably agree to be subject to some types of searches and seizures because they have an interest in reducing the level of crime, and permitting searches facilitates that goal. But they presumably also value freedom from capricious police conduct, and so would insist on some level of cause to justify intrusive police actions, and might bar some types of police action altogether." (quoting William J. Stuntz, *Implicit Bargains, Government, Power, and the Fourth Amendment*, 44 STAN. L. REV. 553, 562 (1992))).

the courts: prohibiting the use of the plain view doctrine in digital searches, unless the search is for evidence of a limited number of "flagged crimes"—sex crimes, crimes against children, or serious felonies.

Whereas most of the distinctions drawn by courts and commentators in evaluating digital searches depend on factors like the intent of the investigator[179] or the search methodologies used,[180] this solution divides all searches into one of two categories: searches for flagged crimes and searches for everything else. Flagged crimes are those crimes that are inherently similar to child pornography—a serious and prevalent cybercrime[181]—and an enumerated number of particularly serious core felonies (e.g. rape, murder, terrorism).[182] When any of these crimes appear in the search warrant, the plain view doctrine will remain intact and will continue to operate in the way it does presently. For all other crimes, however, the plain view doctrine will be unavailable to investigators, thereby prohibiting the use of any incriminating evidence that is not within the warrant.[183] It is the nature of the crime, then, and not the investigator's behavior, that drives this analysis.

The nature of the crime investigated is a variable that has historically been excluded from Fourth Amendment analysis.[184] The Fourth Amendment is thought to be "trans-substantive," meaning that it applies with equal force to all categories of crimes.[185] Although the nature and severity of the crime intuitively seems relevant to how we should evaluate what is an appropriate and reasonable search, courts rarely make mention of that aspect,[186] creating what one scholar has described as "a gulf between actual reasonableness and doctrinal

---

179. *See supra* Section III.B.ii.

180. *See supra* Section III.B.iii.

181. *See* Richard Wortley & Stephen Smallbone, *Child Pornography on the Internet*, CENTER FOR PROBLEM-ORIENTED POLICING (2006), http://www.popcenter.org/problems/child_pornography/1#endref18 ("[A]ll of the available evidence points to [Internet child pornography] being a major and growing problem.").

182. *See* Bellin, *supra* note 10, at 26–33 (describing a "crime hierarchy" including the most serious "grave crimes").

183. The inevitable discovery and independent source doctrine would still apply, permitting some extra-warrant evidence.

184. Bellin, *supra* note 10, at 7–8.

185. *Id.* at 4 (quoting William J. Stuntz, Commentary, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 869 (2001)).

186. *Id.* at 11 ("In the vast majority of cases, the Supreme Court, and thus lower courts, simply ignore the underlying crime in assessing the reasonableness of a search or seizure.").

reasonableness."[187] By incorporating the nature of the crime into the applicability of the plain view doctrine, this solution is not only consistent with public intuitions about the importance of crime severity,[188] but it empowers courts to heighten privacy rights without significantly impeding government investigations of serious crimes.

The mechanics of incorporating the nature of the crime into a digital-search doctrine are relatively simple. First, the crime evaluated would need to be the crime in the warrant and, to the extent that the two might differ, not the crime that is ultimately charged. As the solution aims to regulate the behavior of the investigator at the time of his investigation, it must be based on the information available to the investigator when the investigation begins.[189] Second, the actual crimes to be labeled as flagged must be specifically enumerated to ensure that the solution is predictably and universally applied.[190] This Note suggests three categories of flagged crimes: crimes of a sexual nature, crimes against children, and serious felonies. The first two of these are relatively contained and could easily be filled according to the statutory description of the crime.

Defining which felonies are serious, however, has proven to be a sticking point for courts that have considered adding crime severity into their Fourth Amendment jurisprudence because it can be prohibitively difficult to design a principled method for distinguishing the severity of crimes.[191] Professor Jeffrey Bellin's proposal to define serious crimes by reference to the opinions of the reasonable person, however, is an effective and workable answer.[192] As Professor Bellin notes, the literature supports that there is widespread societal agreement about the relative seriousness of a variety of different crimes, which can provide an appropriate basis for categorizing offenses.[193] Furthermore, the Supreme Court already appeals to community norms in its Fourth Amendment analysis; for instance, in deciding whether a Fourth Amendment "search" has even occurred in the first place, it instructed courts to ask whether the searched

187. *Id.* at 5. (quotation marks omitted).

188. *Id.* at 9.

189. *Id.* at 23.

190. *Id.* at 26.

191. *Id.* at 13–14.

192. *Id.* at 29.

193. *Id.* at 30 ("While views as to *absolute* severity vary among social groups, social-science literature points to 'the existence of wide general agreement and stability across different social sectors and population groups with regard to the relative seriousness of behaviors considered to be criminal."). (citation omitted).

individual had a "reasonable expectation of privacy."[194] This jurisprudence suggests that the Court may be comfortable defining serious crimes by reference to the opinions of a reasonable person, and accordingly, that this is a realistic way for judges to determine those crimes that society believes should be investigated more thoroughly.[195] In this context, investigating thoroughly means having access to the plain view doctrine.

The central benefit of eliminating the use of the plain view doctrine for the investigation of most crimes is the added privacy protections it affords suspects. With the knowledge that incriminating evidence outside the warrant will be inadmissible, investigators might be less likely to conduct broad searches. This solution also reduces the incentive to conduct pretextual searches, as most searches will not be able to return evidence of a crime outside the warrant.

Additionally, this solution is a feasible one for the Court. Because the plain view doctrine is judicially created, and not part of the text of the Fourth Amendment, restricting its use may be more appealing than solutions that require reinterpretation of the Constitution. When compared to attempts to incorporate the nature of the crime into judicial analyses of "reasonable" or "particularity"—operative language in the Amendment—abrogating the plain view doctrine in a relatively small subsection of searches is considerably less disruptive, and thus more feasible for the judiciary.

Obviously, this solution has attendant drawbacks, as gains in privacy are necessarily traded for losses in investigative maneuverability. Here, an investigator's ability to use evidence in plain view during a digital search is sacrificed for additional privacy protections. Ideally, this sacrifice would not be necessary. However, by allowing the plain view doctrine for those searches that are most likely to reveal evidence of more serious crimes, this solution attempts to mitigate the effect of that sacrifice. Notably, when the Ninth Circuit briefly eliminated the availability of the plain view doctrine for *all* digital searches, the government was largely concerned with how that restriction would inhibit its ability to investigate serious crime like terrorism and child rape.[196] By retaining the plain view doctrine for

194. *Id.* at 29.

195. Additionally, Professor Bellin emphasizes that these crimes must be judicially determined, as legislative determination could result in inconsistent application or manipulation, and because the judiciary is charged with interpreting the proper bounds of the Fourth Amendment. *Id.* at 27–28.

196. *Id.* at 43.

those types of investigations, this solution eliminates that concern. Furthermore, it does so without infringing upon the Fourth Amendment rights of suspects of flagged crimes. Those suspects will still receive the full protection of the Fourth Amendment—the reasonableness and warrant requirements will continue to apply with full force—but will receive fewer protections than the suspects of all other crimes. Operating under the premise that some sacrifice is necessary to ensure greater privacy rights, this seems like the least painful sacrifice available.

Another potential pitfall of this solution concerns problems surrounding the designation of flagged crimes. While reference to the reasonable man provides a good foundation for categorizing crimes, disagreements about particular offenses and whether crime distinctions are defensible could strain the process. As previously mentioned, this is an "administrability" problem that is at the heart of the Court's objection to crime-severity analysis.[197] These disagreements are not fatal to this solution. First, crimes of a sexual nature and crimes against children are finite and easy to recognize, and to the extent that particular crimes in these categories do not seem to fit, exceptions can be made via the common law process. Second, because the "serious felony" category of flagged crimes purports to include only those crimes that are universally reviled, there is unlikely to be much, if any, disagreement among the "reasonable community." Indeed, if there is no general consensus about the gravity of a particular felony, it would probably not be appropriate to include that felony in the flagged-crimes category.

Finally, because this solution does not strip any suspects of Fourth Amendment protections, but merely provides the *additional* protection of eliminating the plain view doctrine for investigations of most crimes, shortcomings in the designation process are not as worrisome as they would be in other contexts. For example, Professor Bellin has suggested incorporating crime severity into the analysis of what is a reasonable search,[198] prompting concerns that this will lead to a regime where warrants are required for minor crimes, but searches for evidence of serious crimes can be reasonably conducted

197. *Id.* at 13.

198. *See generally id.* (arguing for an increased role for crime severity in Fourth Amendment jurisprudence).

without a warrant.[199] By contrast, this solution only implicates the use of the plain view doctrine and will have no impact on the warrant or reasonableness requirements. Regardless of the nature of the crime investigated, investigators will need a warrant supported by probable cause and particularity, and will need to adhere to a level of reasonableness that is applied to all searches. Accordingly, even if a borderline crime were included in the flagged-crimes category, the suspect would be in no worse a position than he would be if this solution were not implemented; the plain view doctrine would merely apply to the search of the suspect's property, just as it always had. The significance of any missteps in the designation process, therefore, is limited by the fact that this solution cannot strip from suspects any of their Fourth Amendment protections.

Digital searches can expose investigators to enormous amounts of personal data that would not be uncovered by physical searches, and it is against this backdrop that this solution should be considered. By abandoning the plain view doctrine for digital searches except in the case of flagged crimes, significant privacy gains are made without impeding important investigations. There are shortcomings to this solution, but the sacrifices it entails are made by the state and not the suspect, which seems like the appropriate response in light of the original problem. The solution then, while imperfect, helps to alleviate the significant privacy concerns that surround this area of the law.

V. CONCLUSION

As technology continues to play a larger role in society, the privacy and security of our digital files will become increasingly important. For over two hundred years, the Fourth Amendment has provided the framework necessary to protect Americans from intrusive government searches and seizures. In light of the unique set of problems and considerations presented by digital searches, however, there is reason to believe that the existing framework is no longer sufficient. By limiting the use of the plain view doctrine to digital searches conducted for a limited set of crimes, this solution helps ensure that comprehensive digital-search techniques will not eviscerate the protections of the Fourth Amendment.

---

199. Christopher Slobogin, *Why Crime Severity Analysis is Not Reasonable – A Comment on Jeffrey Bellin, Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. BULL. 1, 2 (2012).

The solution is not without its drawbacks, and situations will arise where it prevents investigators from using clear evidence of a crime. Any solution that increases privacy rights will involve an attendant decrease in state power, however, and by factoring in the nature of the crime in the warrant, this solution will mitigate the impact of that decrease. By merely eliminating the plain view doctrine in certain circumstances, this solution does not reduce the Fourth Amendment rights of suspects of serious crimes, but adds to the protections of those suspected of minor crimes. Relative to the status quo, then, no suspects are hurt by the solution, and many are benefited. By no stretch will this solution be a panacea that protects against all governmental violations of digital privacy rights, but in light of the current shortcomings in how the Fourth Amendment applies to digital searches, it represents a significant step in the right direction.

Eric Yeager[*]

[*] Candidate for Doctor of Jurisprudence, May 2013, Vanderbilt University Law School. I would like to thank the editorial staff of the VANDERBILT LAW REVIEW for their recommendations and editing assistance. I am also grateful to my parents, who provided continued support and guidance throughout the writing process.