EXECUTING WARRANTS FOR DIGITAL EVIDENCE: THE CASE FOR USE RESTRICTIONS ON NONRESPONSIVE DATA

Orin S. Kerr[*]

Abstract

This Article considers how the Fourth Amendment should limit the process of executing search warrants for digital evidence. Warrants for digital evidence are normally executed in two stages. First, agents enter the physical place to be searched and seize all computers. Second, agents conduct an electronic search for the responsive data described in the warrant. The two-stage process raises the prospect that warrants for digital evidence will be executed in ways that resemble general warrants. If agents can seize everything at the first stage, and see all the data at the second stage, what stops agents from accessing and using a target's entire digital world every time a computer warrant is executed?

This Article argues that the Fourth Amendment should be interpreted to impose a use restriction on nonresponsive data seized during the execution of computer warrants. After reviewing the various ways courts could limit the execution of computer warrants, it concludes that use restrictions are the best way to restore the traditional limits on searches for the new technological environment of computers. The Article then revisits the Author's earlier conclusion that courts can achieve that result by eliminating the plain view exception for computer searches. While still a possible approach, eliminating the plain view exception raises underappreciated doctrinal puzzles.

The better path is for courts to rule that the Fourth Amendment imposes use restrictions on nonresponsive data because use transforms the underlying seizure from a justified and modest step needed to execute the warrant to an unjustified and invasive seizure unrelated to the warrant itself. Agents can overseize at the first stage because they must, and they can search through all the data for the responsive files because there is no other way to ensure that they find all the evidence described in the warrant. But when agents use nonresponsive data, the seizure of that data is no longer justified by the warrant and ordinarily is no longer reasonable. This approach also

---

* Fred C. Stevenson Research Professor, George Washington University Law School. This Article is loosely based on the keynote address I delivered at the Texas Tech School of Law Criminal Law Symposium, *The Fourth Amendment in the 21st Century*, on April 17, 2015. Thanks to Scott Greenfield and my fellow participants at the Symposium for thoughtful questions and comments on an earlier draft.

allows courts to impose an exigent circumstances exception to the use restriction: When a review of nonresponsive files reveals exigent circumstances, agents can use the nonresponsive files to address the exigency.

I. INTRODUCTION

The last thirty years have witnessed the emergence of a new kind of Fourth Amendment search: Searches for digital evidence from electronic storage devices.[1] The new searches raise challenges for Fourth Amendment law because of the technological facts of computer storage. This Article explores one of the most important questions raised by these technological

1. In this Article, I use the terms *computer* and *digital storage devices* interchangeably. I mean to refer broadly to storage devices that can contain digital evidence, which might include computers, devices that contain electronic storage devices, and dedicated storage devices such as flash drives or backup hard drives.

changes: What will limit the scope of digital evidence searches authorized by warrants?

The relevant technological facts are easy to grasp. A typical person today owns many electronic storage devices. Each device can store hundreds of thousands or even millions of pages worth of information.[2] It is impossible to know if specific information is contained on a device without searching it. And behind the scenes, it turns out that electronic information can be stored anywhere on a device.[3] Putting these facts together, a law enforcement search for digital evidence requires searching for a needle in an enormous electronic haystack. And because computers get better and better every year, storing more and more information, the haystack is becoming exponentially larger over time.[4]

These technological facts will have major consequences for Fourth Amendment law. The core historical role of the Fourth Amendment was to prohibit general warrants, which are warrants that do not state with particularity where the warrant can be executed and what items the agents can search for and seize.[5] The idea was to limit the scope of warrant searches by limiting where agents can go and what they can take.[6] The facts of computer storage threaten that limiting role.[7] They create the prospect that computer warrants that are specific on their face will resemble general warrants in execution simply because of the new technological environment.[8]

If the government must search the entire electronic haystack for the needle, and agents may see all the information the haystack reveals along the way, how is the execution of a computer warrant different from the execution of the general warrants that the Fourth Amendment was enacted to prohibit? Are new limits required on the computer search warrant process to restore the traditional limits on warrant searches? If so, what limits are appropriate, and what doctrinal path should courts take to impose them?

I first addressed these issues a decade ago in an article titled *Searches and Seizures in a Digital World*.[9] I reluctantly concluded that the best way

---

2. Just to pick an example, a flash drive that many people today carry in their pockets or in their bags might typically store in the range of 8 gigabytes to 256 gigabytes. *See, e.g.*, *Mobile Storage*, SANDISK, http://www.sandisk.com/products/usb/drives/ (last visited Sept. 29, 2015). A single gigabyte of storage is estimated to contain the equivalent of about 65,000 pages worth of Microsoft Word documents. *See How Many Pages in a Gigabyte?*, LEXISNEXIS, http://www.lexisnexis.com/applied discovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf (last visited Sept. 29, 2015). Putting the pieces together, a single 256-gigabyte flash drive could store over 16 million pages of Microsoft Word documents. *See id.*; *Mobile Storage*, *supra*.

3. *See infra* Part II.A.

4. *See* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 302 (2005) [hereinafter Kerr, *Digital Evidence*].

5. *See* Stanford v. Texas, 379 U.S. 476, 480–86 (1965).

6. *See id.*

7. *See infra* Part III.

8. *See infra* Part III.

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

to limit computer searches was to narrow or even eliminate the plain view exception for digital searches.[10] The idea was to restore the limits of particular searches *ex post* by barring the seizure of information outside the scope of the warrant.[11] That recommendation came at the end of the article, and it remained somewhat tentative and unexplored.[12] Back then, I wrote that "eliminating the plain view exception would be too severe at present," but that it may be necessary "[a]s time passes."[13] A decade of time has since passed, prompting me to revisit the question with the benefit of that experience.

This Article argues that it is time for courts to interpret the Fourth Amendment as imposing a use restriction on nonresponsive files seized during the execution of a warrant for digital evidence. Interpreting the Fourth Amendment as imposing a use restriction on nonresponsive data seized under a warrant can restore the needed limits on the warrant authority in light of the new facts of computer searches.[14] This interpretation achieves two essential goals at once. First, it maintains the efficacy of searches by providing the government the needed authority to search for and seize evidence described in a proper warrant.[15] Second, it avoids general warrants by limiting the government to the particularly described evidence or contraband that the government has established probable cause to seize.[16] The result maintains the original goals of the Fourth Amendment's Warrant Clause in the new digital environment.

This Article then considers how courts should impose a use restriction. Under the first path, one I first explored a decade ago, courts would hold that the plain view exception applies in searches for physical evidence but does not apply to searches for digital evidence.[17] This approach has considerable merit, especially in light of the computer-specific approach to the Fourth Amendment adopted by the Supreme Court in *Riley v. California*.[18] At the same time, relying on the plain view exception ends up raising two doctrinal puzzles that may give courts pause.[19] A close look at the facts of computer searches suggests that whether agents can use nonresponsive data may not be a plain view question at all.[20] Plain view might not be the problem, and eliminating plain view might not be the answer.

---

10. *See id.* at 582–84.
11. *See id.*
12. *See id.* at 584.
13. *Id.* at 583.
14. *See infra* Parts IV–V.
15. *See infra* Part III.D.
16. *See infra* Part III.D.
17. *See infra* Part IV.A.
18. *See* Riley v. California, 134 S. Ct. 2473, 2493–94 (2014).
19. *See infra* Part IV.
20. *See infra* Part IV.B.

This Article then develops a better path that it terms the "ongoing seizure" approach. Courts should hold that using nonresponsive files seized during the execution of a two-stage computer warrant renders the seizure of those files constitutionally unreasonable.[21] Although the initial overseizure of nonresponsive files and search through those files is reasonable because investigative necessity demands it, subsequent use of nonresponsive files transforms the nature of the government's interference with the owner's possessory interests.[22] Under the ongoing seizure approach, the government normally can only seize and view nonresponsive files; it cannot then use those files as if they had been articulated in the original warrant.[23] This approach results in the same use restriction that could be achieved by eliminating the plain view exception.[24] At the same time, it does so in a narrower and simpler way that has stronger support in existing precedent.[25]

Judicial imposition of use restrictions on nonresponsive data in computer warrant cases raises difficult questions about the proper scope of the limitation. For example, what exactly constitutes "use"? Does mere disclosure count? Another question, raised in a case pending before the en banc Second Circuit, is whether the use restriction should only bar use of nonresponsive data revealed in executing the warrant or whether it should also bar the execution of additional warrants based on independent probable cause.[26] This Article flags these difficult issues but does not resolve them. It does address one important question about scope, however: A proper use restriction can include an exigent circumstances exception permitting use when review of nonresponsive files reveals an exigency.[27]

The Article proceeds in five parts. Part II reviews the current law and practice governing the execution of computer warrants. Part III argues that a doctrinal shift is necessary to impose new limits on computer warrant searches, and that the limit should come in the form of use restrictions on nonresponsive data. Part IV considers how courts might implement use restrictions using the plain view exception. Part V explores the easier alternative of the "ongoing seizure" approach. Part VI shows how courts could adopt an exigent circumstances exception to the use restriction.

---

21. *See infra* Part V.A.
22. *See infra* Part V.A.
23. *See infra* Part V.A.
24. *See infra* Part V.A.
25. *See infra* Part V.B.
26. *See* United States v. Ganias, 755 F.3d 125, 137–38 (2d Cir. 2014), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015) (reheard en banc Sept. 30, 2015).
27. *See infra* Part VI.

II. EXISTING LAW ON EXECUTING WARRANTS FOR DIGITAL EVIDENCE

The execution of warrants for digital evidence ordinarily divides into two stages.[28] First, during the physical search stage, agents search for and seize electronic storage devices such as computers and any storage disks that may contain the evidence sought.[29] Second, during the electronic search stage, agents make copies of the data contained in the seized storage devices and then use forensic software to search the copied data for the evidence described in the warrant.[30]

The law regulating this process must address three major questions. First, during the physical search stage, what limits an officer's ability to seize physical storage devices for later analysis? Second, during the electronic search stage, what limits an officer's ability to comb through the electronic files for evidence? And third, after the electronic search stage, what limits an officer's ability to use information discovered during the electronic search stage?

A. The Physical Search Stage

Current law on the physical search stage is simple and deferential to law enforcement. When officers execute a warrant for digital evidence, courts have held that the officers can remove any computers that might contain the digital evidence described in the warrant.[31] They can then take the computers off site for a subsequent search.[32] Rule 41 of the Federal Rules of Criminal Procedure now expressly recognizes the need for two-step computer seizures.[33] The Committee Notes to the 2009 rule change state:

> Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.[34]

---

28. *See* Orin S. Kerr, *Search Warrants in An Era of Digital Evidence*, 75 MISS. L.J. 85, 86–87 (2005) [hereinafter Kerr, *Search Warrants*].

29. *See id.*

30. *See id.*

31. *See, e.g.*, United States v. Hill, 459 F.3d 966, 973–75 (9th Cir. 2006); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (stating that the "narrowest definable search and seizure reasonably likely to obtain" the evidence sought will generally be "the seizure and subsequent off-premises search of the computer and all available disks").

32. *Upham*, 168 F.3d at 535.

33. FED. R. CRIM. P. 41(e)(2) advisory committee's notes to 2009 amendments.

34. *Id.*

As this passage suggests, allowing the physical seizure of storage devices at the initial physical search stage has been justified by practical concerns.[35] A place to be searched can contain many electronic storage devices, and the evidence could be anywhere inside any device. The electronic search stage can be extremely time-consuming even for one device.[36] Given these realities, courts have reasoned, the only way to ensure a relatively brief search at the physical search stage is to allow officers to remove storage devices and search them off site later on.[37]

Courts have not identified substantive limits to this permissive approach. The Ninth Circuit stands alone in adding a procedural requirement: Agents must explain the need for the overseizure in the warrant affidavit.[38] But this requirement is modest in practice, in part, because the need normally arises in every computer search case, and the exclusionary rule does not apply if agents fail to do so.[39]

B. The Electronic Search Stage

The next step is the electronic search stage. In the typical case, agents will bring the devices off site and make a perfect electronic copy of the device.[40] The perfect copy, known as an "image," exactly replicates what is on the original.[41] Agents will then run forensic software on the image in a search for digital evidence.[42] The goal of the electronic search is to identify the data that is responsive to the warrant—that is, the data that falls within the particular description of the property to be seized.[43] The responsive data can then be separated out from the nonresponsive data outside the scope of the warrant.[44]

Courts are generally deferential in allowing agents the discretion to find adequate ways to identify the responsive data. As long as agents search in a reasonable fashion, most courts say the search is proper.[45] There is no clear case law, at least yet, on the outer bounds of when a search for responsive data at the electronic search stage becomes "unreasonable." Some courts

---

35. *See id.*
36. *See Hill*, 459 F.3d at 973–75.
37. *See id.*; *see also* United States v. Schandl, 947 F.2d 462, 465–66 (11th Cir. 1991) (suggesting that an on-site search "might have been far more disruptive" than seizing the computers and searching them off site).
38. *See Hill*, 459 F.3d at 975 ("Although computer technology may in theory justify blanket seizures for the reasons discussed above, the government must still demonstrate to the magistrate *factually* why such a broad search and seizure authority is reasonable in the case at hand.").
39. *See id.* at 977.
40. *See* Kerr, *Search and Seizures*, *supra* note 9, at 534.
41. *Id.* at 540–41.
42. *Id.* at 545.
43. *See id.* at 537–38.
44. *See id.* at 536–37.
45. *See, e.g.*, United States v. Johnston, 789 F.3d 934, 941 (9th Cir. 2015).

have indicated that a search becomes unreasonable when an agent subjectively ceases to look for the responsive data and instead begins looking for other data.[46] But other courts reject the subjective approach, instead finding searches reasonable even if they may result in highly invasive forensic searches through the hard drive for evidence outside the scope of the warrant.[47]

An important caveat to this deference is the uncertain legal status of *ex ante* search restrictions.[48] Some individual magistrate judges impose special conditions on the issuance of computer warrants that limit how the search can be conducted.[49] For example, a magistrate judge might impose a "search protocol" that requires the electronic search stage to be conducted in a particular order or with certain limits.[50] The purpose of these restrictions is to narrow computer searches: The magistrate imposes a limit at his or her discretion that the agents must follow as a condition of acquiring the warrant.[51]

Federal circuit courts have rejected the view that search protocols are required, and none have required *ex ante* restrictions for computer warrants.[52] Whether *ex ante* restrictions are even permitted remains uncertain.[53] It is also unclear what remedy applies if an *ex ante* search restriction is violated. Some authority suggests that the remedy is automatic suppression, while other authority suggests that there is no remedy at all.[54]

C. Subsequent Use

The remaining question is whether and when agents can use the information they have viewed in the course of the search. When evidence is

---

46. *See* United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010); United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999). Conversely, when the search appears to have been for the evidence described in the warrant, the search is reasonable. *Johnston*, 789 F.3d at 942–43.

47. *See Johnston*, 789 F.3d at 942–43.

48. *See generally* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1246 (2010) [hereinafter Kerr, *Ex Ante Regulation*] (noting that "*ex ante* regulation of computer warrants" may be unconstitutional).

49. *See id.* at 1248–60.

50. *See id.*

51. *See, e.g.*, *In re* United States' Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius, 770 F. Supp. 2d 1138, 1149–52 (W.D. Wash. 2011).

52. *See* United States v. Evers, 669 F.3d 645, 653 (6th Cir. 2012) (citing United States v. Richards, 659 F.3d 527 (6th Cir. 2011)). The Ninth Circuit briefly embraced a search protocol requirement in its initial en banc ruling in *Comprehensive Drug Testing*, but the opinion was amended to not make this a requirement. *See* United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1178–80 (9th Cir. 2010) (per curiam).

53. Only the Vermont Supreme Court has expressly ruled on this issue. Applying a deferential standard of review, it allowed some *ex ante* restrictions but not others. *See In re* Search Warrant, 71 A.3d 1158, 1170 (Vt. 2012).

54. *Compare id.* at 1164–65 (concluding that violating *ex ante* restrictions violates the Fourth Amendment), *with* Kerr, *Ex Ante Regulation*, *supra* note 48, at 1268–71 (concluding that violating *ex ante* restrictions has no Fourth Amendment relevance).

outside the warrant, this traditionally has been considered an issue for the plain view exception.[55] The idea is that the warrant authorizes the use of the responsive data but does not itself authorize the use of nonresponsive data.[56] If the plain view exception applies, courts have indicated, then the information observed outside the warrant can be used elsewhere and is not subject to suppression.[57]

As suggested above, courts are divided on how the plain view exception applies to computer searches.[58] The Fourth Circuit has held that no special rules are required,[59] while the Tenth and Seventh Circuits have applied a subjective test that focuses on whether the agent was trying to stray outside the warrant.[60] Under the subjective test, evidence discovered outside the scope of the warrant can be used only if the officer was trying to find the evidence described in the warrant when he exposed that additional evidence to his plain view.[61] Finally, the Second Circuit and the Massachusetts Supreme Judicial Court have suggested that they might tighten or eliminate the plain view exception in the future, although neither have reached a clear holding on the question.[62]

The Second Circuit recently imposed a use restriction on overseized files but then vacated the decision pending rehearing en banc. In *United States v. Ganias*, the court held that nonresponsive files overseized out of necessity during the physical search stage must eventually be deleted, or at least not used in other cases, even if the government obtains a second warrant based on fresh probable cause.[63] The vacated decision in *Ganias* acts as an equitable doctrine that counters the deferential standards at the preceding stages.[64] Although the government can overseize at the physical search stage out of necessity, agents cannot take unfair advantage of that overseizure.[65] The nonresponsive files seized only out of necessity are walled off from further use even if they later become important evidence in a new investigation.[66] This panel decision has been vacated pending rehearing en banc, and the en banc court has not yet ruled on the case.[67]

---

55. *See infra* note 122–26 and accompanying text.

56. *See infra* note 126 and accompanying text.

57. *See, e.g.*, United States v. Williams, 592 F.3d 511, 524 (4th Cir. 2010).

58. *See id.* at 522–24; United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010).

59. *Williams*, 592 F.3d at 522–24.

60. *See Mann*, 592 F.3d at 786; United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999).

61. *Mann*, 592 F.3d at 784–85.

62. *See* United States v. Galpin, 720 F.3d 436, 451–52 (2d Cir. 2013); Preventive Med. Assocs. v. Commonwealth, 992 N.E.2d 257, 274 (Mass. 2013).

63. United States v. Ganias, 755 F.3d 125, 137–40 (2d Cir. 2014), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015).

64. *See id.*

65. *Id.*

66. *Id.* at 137–40.

67. *Ganias*, 791 F.3d at 290. The case was reheard by the Second Circuit en banc on September 30, 2015. *Id.*

III. WHAT WILL LIMIT COMPUTER SEARCHES?

In a recent decision, *Riley v. California*, the Supreme Court adopted a new approach to computer search and seizure law.[68] Digital is different, the Supreme Court indicated, because physical-world rules lead to unreasonable results when applied to the new facts of computer searches.[69] I have called this methodology "equilibrium adjustment" because it adjusts Fourth Amendment doctrine to counter new technological facts.[70] If the consequences of an old rule are vastly different when applied to a new and important set of facts, the Supreme Court will often adopt a new rule to restore the equilibrium struck by the old rule in the old factual environment.[71] As a result, computer technologies can call for computer-specific rules.

After *Riley*, we can call judicial adoption of a new rule to adjust the equilibrium for computer searches a "*Riley* moment." I expect that *Riley* is just the first in a series of *Riley* moments when the Supreme Court recognizes that the facts of computer searches differ so greatly from the facts of physical searches that new rules are required. New facts demand new law to restore the function of the old law in the new technological environment. Equilibrium adjustment, as shown in *Riley*, can and should point the way forward to new rules for applying the Fourth Amendment in digital evidence cases.[72]

The facts of computer warrant searches call for another such *Riley* moment. Current law allows computer searches for any evidence to look disturbingly like searches for all evidence.[73] Everything can be seized.

---

68. Riley v. California, 134 S. Ct. 2473, 2493–94 (2014). The Court technically spoke of "cell phones," the type of computer that was at issue in the two consolidated cases before the Court. *Id.* But the Court made clear that its analysis is really about computers generally, not just computers that allow voice transmission and are therefore called phones. *See id.* at 2489 ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone.").

69. *Id.* at 2488. The key passage was the following:

> The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches . . . of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

Id. at 2488–89 (citation omitted).

70. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

71. *See id.* at 487–90.

72. *See Riley*, 134 S. Ct. at 2493–94.

73. *See* United States v. Ganias, 755 F.3d 125, 136 (2d Cir. 2014) (citing United States v. Shi Yan Lieu, 239 F.3d 138, 140–41 (2d Cir. 2000)), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015).

Everything can be searched. Nearly everything can come into plain view and be subject to use in unrelated cases. The result seems perilously like the regime of general warrants that the Fourth Amendment was enacted to stop.

But if a *Riley* moment is called for, the hard question is how to do it. "Digital is different" is a slogan rather than a guide. If courts should change Fourth Amendment doctrine to restore the limits of search warrants, what change or changes should they make? Like most difficult legal questions, no perfect answer exists. The challenge is to identify the least bad answer among the alternatives. We can do that by identifying the doctrinal pressure point that best reflects the Fourth Amendment directive that searches and seizures should be constitutionally reasonable.

In my view, the doctrinal change should be to impose a use restriction on nonresponsive data obtained pursuant to a warrant. Agents should be allowed to overseize at the physical search stage and conduct a comprehensive search at the electronic search stage. But in general, the government should only be limited in what they can then use based on what is actually responsive to—that is, described by—the warrant. This approach best reconciles the government's compelling need to obtain the evidence sought in the warrant with the Fourth Amendment's prohibition on general warrants. To see why, let's run through each of the stages in turn.

A. Limits at the Physical Search Stage?

First, courts should not impose limits at the physical search stage. It is true that allowing a full seizure at the physical search stage technically permits an overseizure.[74] The government seizes not just the evidence described in the warrant, for which a judge found probable cause, but also the nonresponsive data that happens to be stored alongside it and any physical devices that might contain it.[75] But there is no reasonable alternative given the time-consuming nature of electronic searches.

The massive storage capacity of computers, combined with the ease of hiding evidence inside them, ensures that computer searches will usually take a lot of time.[76] If the government must find a needle in the haystack, and searching the haystack may take weeks or longer, the government must choose among three unhappy choices. First, they can seize the entire haystack for subsequent searching off site. Second, they can bring a few officers to the haystack and have them stay there for a few weeks as they search through it. Or third, they can simply accept that haystack warrants cannot be executed because haystack searches are too time-consuming. Among these three choices, the first is the least bad option.

---

74. *Id.*

75. *Id.*

76. *See In re* United States' Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius, 770 F. Supp. 2d 1138, 1144 (W.D. Wash. 2011).

Imagine the situation for an agent tasked with finding a particular fraud record that is believed to be at the suspect's home. The agent might enter the home and find a dozen computers, five backup hard drives, ten flash drives, and 100 CD-ROMs. The officer can't know where the record might be without taking the time to go through the devices. Each device might contain an ocean of information using a different operating system or using various tools to hide data. Searching any one device can be quite time-consuming. Searching all of them is much more so. In this context, allowing the agents to seize all the computers and search them off site is the least bad among the bad options that the technology creates.

Perhaps someday the technology will evolve to allow quick searches through electronic storage devices. Based on current technology, however, the time-consuming nature of electronic searches requires allowing seizures of all digital storage devices at the physical search stage.[77] Even if there are some cases where, with the benefit of hindsight, it might have been possible to search quickly onsite, that is a difficult judgment call that officers in the heat of the moment executing the warrant cannot readily be required to make.[78]

Agents may also take steps to minimize the disruption of the all-seizure rule. For example, agents sometimes can make copies of particularly important files or storage devices and either leave the copies behind or send them later.[79] In cases not involving child pornography, agents may also be able to make copies and take only the copies, leaving the physical devices behind.[80] Courts should be reluctant to require such steps in light of the uncertainty of knowing whether copies can be made on site. Law enforcement resources vary widely, and every case is different. The matter is better regulated by statutory warrant rules than the Fourth Amendment.[81] Nonetheless, such commendable steps can minimize the disruption caused by the all-seizure rule.

The Ninth Circuit has allowed two-stage computer searches but requires agents to explain the two-stage search process.[82] The explanation requirement is a mistake, and other courts should not follow it. In 2006, when the Ninth Circuit imposed the requirement, perhaps some judges were

---

77. *See* Kerr, *Search Warrants*, *supra* note 28, at 110–12.

78. *See* Groh v. Ramirez, 540 U.S. 551, 568 (2004) (Kennedy, J., dissenting) (noting than an officer executing a warrant must "protect[] officer safety, direct[] a thorough and professional search for the evidence, and avoid[] unnecessary destruction of property," all of which "demand the officer's full attention in the heat of an ongoing and often dangerous criminal investigation").

79. *See* Kerr, *Search Warrants*, *supra* note 28, at 129–32 (proposing that statutory warrant rules should require officers to make copies of digital files).

80. *See id.* It would of course be inappropriate for the government to make an extra copy of contraband and leave the original contraband behind, together with the instrumentality of the crime that is the physical device.

81. *See id.*

82. *See supra* Part II.A (discussing United States v. Hill, 459 F.3d 966, 973–75 (9th Cir. 2006)).

sufficiently unfamiliar with the two-stage nature of computer searches to make an explanation helpful. Today, however, all magistrate judges and most appellate judges presumably are familiar with the two-stage process. The Federal Rules of Criminal Procedure acknowledge the need for it, and that need arises in most computer search cases.[83] As a result, it is hard to discern what purpose an explanation requirement might serve. The explanation doesn't tell anyone anything they don't already know.

If courts do end up imposing limits on the physical search stage, the limits presumably would be in rare cases involving seizures of third-party servers that might contain records belonging to many nontargets. In such cases, the server owner may be an innocent third party who will cooperate fully with the agents and allow a targeted search without the need for off-site review of hardware.[84] Whether the Fourth Amendment imposes any limits at all in light of the third-party harms remains uncertain.[85] The issue is not likely to arise often in practice, however, as agents have every incentive to work with innocent third parties to conduct a more targeted search where one is possible.[86]

B. Ex Ante *Search Restrictions?*

I also stand by my conclusion, articulated at length in my article *Ex Ante Regulation of Computer Search and Seizure*, that courts should not encourage or allow *ex ante* restrictions imposed by individual magistrate judges.[87] As I have explained, a magistrate judge asked to review a warrant application has no way to know *ex ante* what ways of executing the warrant will end up being constitutionally unreasonable.[88] Allowing every magistrate judge's best guess about what might end up being a good rule of reasonable conduct to govern the execution of the warrant allows individual magistrates to impose their own arbitrary restrictions.

Of course, the Fourth Amendment must impose limits on the execution of warrants. The limits should be recognized by appellate courts exercising

---

83. *See supra* note 33.

84. *See, e.g.*, United States v. Bach, 310 F.3d 1063, 1068 (8th Cir. 2002) (exemplifying cooperation between government agents and private internet service providers under the Stored Communications Act); *see* 18 U.S.C. 2703 (2006).

85. *Cf.* United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1167 (9th Cir. 2010) (en banc) (finding that "the government's actions displayed a callous disregard for the rights of third parties"); *id.* at 1178–83 (Kozinski, J., concurring); *id.* at 1183–85 (Callahan, J., concurring in part and dissenting in part).

86. The relevant cases that might shed light on the question are sparse and mostly decades old, in part because agents now know to work with third parties and to be sensitive to the third-party harms. *See, e.g.*, Davis v. Gracey, 111 F.3d 1472, 1482 (10th Cir. 1997); Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 443–44 (W.D. Tex. 1993), *aff'd on other grounds*, 36 F.3d 457, 463–64 (5th Cir. 1994).

87. *See* Kerr, *Ex Ante Regulation*, *supra* note 48, at 1260–77.

88. *See id.* at 1281–84.

ex post judicial review, however, rather than by magistrate judges *ex ante* in individual warrant applications.[89] When appellate courts review motions to suppress and hand down decisions on the reasonableness of executing warrants, the result is in effect an *ex ante* restriction that applies to every warrant automatically.[90] The government will have to follow those limits as a matter of law in every case. But those limits are wisely imposed by appellate courts after adversarial litigation into Fourth Amendment reasonableness, not by individual magistrate judges simply announcing limits in individual ex parte proceedings with no briefing.[91]

Instead of imposing *ex ante* restrictions, magistrate judges should allow the law of reasonableness to develop in the usual course *ex post*.[92] That would end up imposing rules of reasonableness on all warrants, not just on those individual warrants that happened to have a particular restriction imposed by the magistrate judge.

C. Reliance on the Particularity Requirement?

The next option is relying on the particularity requirement of the Warrant Clause to limit the scope of the search.[93] The particularity requirement limits where officers can search and what officers can search for as a way of limiting how broad the search can be and how much officers can take away.[94] If officers obtain a warrant authorizing them to search a home for a stolen Picasso sculpture, they can only search at that home; once at the home, they cannot look in a place that couldn't fit the sculpture;[95] once the officers find the Picasso, they must stop searching;[96] and unless the plain view

89. *See id.* at 1292–93.

90. *See id.* at 1284

91. *See id.* at 1281–93. *Accord* United States v. Christie, 717 F.3d 1156, 1167 (10th Cir. 2013) ("Unlike an *ex ante* warrant application process in which the government usually appears alone before generalist judges who are not steeped in the art of computer forensics, this *ex post* review comes with the benefit, too, of the adversarial process where evidence and experts from both sides can be entertained and examined.").

92. The Vermont Supreme Court has argued that *ex ante* restrictions do not interfere with the development of reasonableness standards because appellate courts can still review the reasonableness of a warrant search in addition to reviewing compliance with *ex ante* restrictions. *See In re* Appeal of Application for Search Warrant, 71 A.3d 1158, 1172 n.16 (Vt. 2012). This response is inadequate because defense counsel, presented with a plausible violation of an *ex ante* restriction, is unlikely to also press a separate claim that the evidence should be suppressed because the means of executing the warrant was generally unreasonable. Making the reasonableness argument only weakens the *ex ante* restriction claim by reminding the reviewing court that the violation of the *ex ante* restriction did not actually render the search unreasonable. A defense attorney is more likely to only raise the violation of the *ex ante* restriction.

93. The Warrant Clause states: "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." U.S. CONST. amend. IV.

94. *See* Stanford v. Texas, 379 U.S. 476, 480–86 (1965).

95. *See* United States v. Ross, 456 U.S. 798, 824 (1982).

96. *See* Horton v. California, 496 U.S. 128, 141 (1990) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 517 (1971)).

exception applies, officers cannot take other property away. At least in theory, the particularity requirement limits the scope of computer searches.

The big problem is that the particularity requirement does not play the significant role in computer search cases that it can play in physical search cases.[97] First, the place to be searched is no longer a significant limit. A single home, the classic unit of particularity for a place to be searched,[98] could contain thousands of electronic storage devices or servers that can serve hundreds of thousands of people. The requirement that warrants must particularly describe the thing to be seized is the more promising possibility. But it too plays a much more limited role in computer searches than in physical searches.[99]

If particularized evidence can be anywhere in a hard drive, the ability to describe with particularity what agents are looking for no longer places a limit on where they can look for it.[100] If the evidence can be anywhere, agents can look anywhere in the place to be searched to find it.[101] In that sense, digital searches may resemble searches for illegal drugs that can be stored anywhere[102]—with the catch that the place to be searched is the virtual equivalent of a city rather than an individual home.[103] If the place to be searched can store thousands of devices, each device can store libraries of information, and there are no limits on where the evidence might be, the particularity clause no longer does significant work in limiting the scope of digital searches. As I put the point in 2005: "the particularity requirement no longer serves the function in electronic evidence cases that it serves in physical evidence cases."[104] And that is even clearer today given the vastly greater storage capacities of computers in 2015.

The important question is whether the description of digital items to be seized can be sufficiently narrow that the specific description limits the scope of the search for that evidence. Can agents make definitive assessments of where particular evidence will be (if it exists at all), and thus limit their searches to only those places or services on the storage devices? The problem

---

97. *See* Kerr, *Digital Evidence*, *supra* note 4, at 302–03, 314.

98. *See* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.5(a) (5th ed. 2012).

99. *See* Kerr, *Digital Evidence*, *supra* note 4, at 303.

100. *Id.* at 302–03 ("Given how much information can be stored in a small computer hard drive, the particularity requirement no longer serves the function in electronic evidence cases that it serves in physical evidence cases.").

101. *See* United States v. Ross, 456 U.S. 798, 820–21 (1982).

102. As indicated by the many Fourth Amendment cases involving drugs hidden in cars, drugs can be hidden in some surprising places. *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 150 (2004) (drugs hidden in fake gas tank); United States v. Guevara, 731 F.3d 824, 826 (8th Cir. 2013) (drugs hidden inside engine); United States v. Davila-Escovedo, 36 F.3d 840, 842 (9th Cir. 1994) (drugs hidden in walls of truck).

103. *See* Kerr, *Digital Evidence*, *supra* note 4, at 303 ("Today, limiting a search to a particular computer is something like limiting a search to a city block; ten years from now, it will be more like limiting a search to the entire city.").

104. *See id.*

is a practical one. If descriptions of what the agents are looking for are so limited that the electronic stage search only reveals a small amount of information on the device, then perhaps the particularity of the items sought will result in narrow searches. In that case, particularity alone might limit the scope of computer searches without the need for a *Riley* moment. On the other hand, if such limits are not likely in practice, then the particularity requirement alone is insufficient.

Consider the example of date restrictions. Imagine agents are investigating a fraud scheme involving a document that the agents know was created on June 19, 2012. On a typical computer running a Windows operating system, the operating system saves a record for each file of when the file was created, accessed, and modified.[105] If agents obtain a warrant for that one document, and they can limit their searches to files created on that date, then perhaps agents can execute a narrow search because their search will only reveal the files with that date. If that is possible, then particularity will limit the scope of computer searches without the need for reforms elsewhere.

Although this sounds promising in theory, I fear it doesn't work in practice. To be sure, agents sometimes will have ways of targeting searches that will often succeed. If agents are looking for a specific file with a known date, for example, they could start their search by using the known name or date parameter. If they find the file quickly, the search can be over and it will have been a limited search indeed. The problem is that if the file isn't there, the agents cannot know with certainty if the file is not on that device or is simply marked in a way that their search query won't find it.[106] Data can always be changed. Maybe the modification will be easy or maybe it will be hard. But it can always be done. As a result, a negative result for a particular query never offers complete assurance that the evidence isn't there.[107]

Return to the date restriction in my hypothetical above. The suspect can easily use *BulkFileChanger*, a software program that anyone can download from the Internet for free.[108] Using the program, he can change the "date created" entry for that file to any arbitrary value.[109] The suspect might change the date from June 19, 2012 (the real date) to something like May 2, 1982.[110] A search for files created in 2012 will miss it. As a result, even a narrow

---

105. *See, e.g.*, *Dates: NTFS Created, Modified, Accessed, Written*, WHERE IS YOUR DATA?, https://whereismydata.wordpress.com/2009/02/14/dates-ntfs-created-modified-accessed-written/ (last visited Sept. 29, 2015).

106. *See* Kerr, *Digital Evidence*, *supra* note 4, at 303–05.

107. *See id.*

108. *BulkFileChanger*, DOWNLOAD.COM, http://download.cnet.com/BulkFileChanger/3000-2248_4-75182036.html (last visited Sept. 29, 2015) (available for download).

109. *Id.*

110. Martin Hendrikx, *How to Change Created or Modified Timestamps for Files and Folders*, HOW-TO GEEK (Nov. 30, 2014), http://www.howtogeek.com/203154/how-to-change-created-or-modified-timestamps-for-files-and-folders/.

description of evidence sought in the warrant cannot rule out the need for a more comprehensive search. An unsuccessful query cannot rule out that the evidence is there but not found by the narrow query.[111]

This point is intuitive with physical searches. Imagine agents are looking for a 2010 tax record in a suspect's file cabinet. They find a folder marked "2010 Tax Records." Agents will likely look in that folder first. If the record sought is in the file cabinet, there's a good chance it is in that folder. But if the agents *don't* find the record there, they won't call off the search. The record might be in another folder, either accidentally or by design. Because the legal authority to search the file cabinet extends to the whole cabinet, not just the one folder that is likely to contain the record sought, agents will continue searching. The same principle applies to computer searches. Even evidence that can be described very specifically might be anywhere on the storage device.

The problem is even greater when the description of property to be seized is necessarily general in nature. Imagine the warrant asks for classes of records instead of a specific, known single item. The warrant might seek "images of child pornography" or "records detailing a scheme to submit fraudulent travel receipts." When descriptions are more general, as they often are, the search isn't done when agents find one responsive file. If anything, finding one responsive file suggests that other responsive files are likely elsewhere on the storage device if agents can figure out how to find them. For these reasons, particularity alone is unlikely to provide sufficient limits on computer warrant searches.[112]

D. The Need for Use Restrictions

This brings us to the last stage: The possible imposition of use restrictions. In my view, imposing use restrictions on nonresponsive files is the best way to reconcile the government's need to search for responsive evidence with the Fourth Amendment command to avoid general warrants. In *Andresen v. Maryland*, the Supreme Court noted the "grave dangers" to privacy "inherent in executing a warrant authorizing a search and seizure of a person's papers."[113] "In searches for papers," the Court noted, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."[114] In response, the Court warned, "responsible officials . . . must take care to assure that [the searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy."[115]

---

111. *See* United States v. Richards, 659 F.3d 527, 541 (6th Cir. 2011).
112. *See* Kerr, *Digital Evidence*, *supra* note 4, at 303–05.
113. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).
114. *Id.*
115. *Id.*

The best way to minimize the unwarranted intrusions upon privacy for computer searches is to impose use restrictions on the nonresponsive data revealed in the course of the search. To avoid that warrant being a dead letter, Fourth Amendment rules should give officers the authority needed to find the particularized evidence described in the warrant. On the other hand, to make sure computer warrants do not resemble general warrants in their execution, the agents should only be allowed to use the evidence that is actually described in the warrant. Nonresponsive data found in the course of the search for responsive data should generally be walled off from further use.

As I argued a decade ago, this approach

> would respect law enforcement interests by granting the police every power needed to identify and locate evidence within the scope of a warrant given the particular context-sensitive needs of the investigation. At the same time, the approach would protect privacy interests by barring the disclosure of any evidence beyond the scope of a valid warrant in most cases. It is an imperfect answer, to be sure, but it may be the best available rule.[116]

When I first proposed this answer a decade ago, I noted that it seemed too early for such a "draconian" approach.[117] A decade later, I think the timing is now right. The remainder of this Article considers how courts can interpret the Fourth Amendment to impose the needed use restriction.

IV. THE FIRST PATH: USE IS FORBIDDEN BECAUSE THE PLAIN VIEW EXCEPTION SHOULD NOT APPLY TO COMPUTER SEARCHES

There are two related ways that courts could interpret the Fourth Amendment to impose a use restriction on nonresponsive files. Whether to treat these two ways as distinct paths is a tricky question that rests on some subtle doctrinal distinctions. For analytical purposes, however, it is helpful to treat the two paths separately.

This Part explores the first path, the elimination of the plain view exception for digital searches. I tentatively offered this approach a decade ago in two different articles.[118] Here I summarize the argument and update it in light of *Riley*. This Part also notes a potential drawback to eliminating the plain view exception that I did not appreciate at the time of my earlier writings.[119] A closer look at the facts of computer searches suggests that use restrictions might not be a plain view problem at all.[120] At the very least,

---

116. Kerr, *Searches and Seizures*, *supra* note 9, at 583–84.

117. *Id.* at 582.

118. *See* Kerr, *Digital Evidence*, *supra* note 4, at 314–17; Kerr, *Searches and Seizures*, *supra* note 9, at 582–84.

119. *See* Kerr, *Digital Evidence*, *supra* note 4, at 314–17; Kerr, *Searches and Seizures*, *supra* note 9, at 582–84.

120. *See infra* Part IV.B.

eliminating the plain view exception might raise difficult conceptual questions that have not yet been appreciated.[121]

A. Imposing a Use Restriction By Eliminating the Plain View Exception

The plain view exception allows government agents to seize evidence or contraband without a warrant when agents have viewed it lawfully and its incriminating nature is immediately apparent.[122] The plain view exception does not only apply in the warrant context: It is a general doctrine of Fourth Amendment law.[123] But the exception serves a critical role in the execution of search warrants.[124] Thanks to the plain view exception, agents executing a warrant can seize beyond the items described in the warrant.[125] While agents can seize the responsive property under the authority of the warrant, they also can seize nonresponsive property under the plain view exception when the incriminating nature of the nonresponsive property is immediately apparent.[126]

The plain view exception plays an important role in the execution of computer warrants because so much information outside the warrant comes into plain view. In a sense, the combination of broad computer searches and the plain view exception is what causes the problem of general-warrant-like searches. The technology lets the government *see* everything, and the plain view exception then lets the government *use* (almost) everything. Courts can respond to the technologically broad scope of computer warrant searches by eliminating the plain view exception that allows the subsequent use of nonresponsive data.

Although I argued for this position long before *Riley*, the *Riley* case now provides significant additional support.[127] Recall that *Riley* allowed broad, warrantless physical searches incident to arrest but introduced a new rule barring those warrantless searches in the computer context given the very different facts of computer searches.[128] An analogous step for plain view would allow broad plain view seizures for physical searches—as current doctrine permits—but bar them in computer searches.

The argument is based on a technological shift much like that in *Riley*. As was the case with the search incident to arrest doctrine considered in *Riley*,

---

121. *See infra* Part IV.B.

122. *See generally* LAFAVE, *supra* note 98, § 6.7(a)–(b) (explaining the development of the plain view exception).

123. *See, e.g.*, Arizona v. Hicks, 480 U.S. 321, 326 (1987) (applying the plain view exception in the context of a warrantless search based on exigent circumstances).

124. *See* LAFAVE, *supra* note 98, § 6.7(b).

125. *Id.*

126. *Id.*

127. Kerr, *Digital Evidence*, *supra* note 4, at 314–17; Kerr, *Searches and Seizures*, *supra* note 9, at 582–84.

128. *See* Riley v. California, 134 S. Ct. 2473, 2488–89 (2014).

the existing broad plain view doctrine was premised on a very different set of facts.[129] The Supreme Court has allowed a broad plain view exception in the physical search context because the particularity requirement limits the scope of searches and officers can only look where the evidence is stored.[130] These limitations are substantial in the context of physical searches. But that is not the case with computer searches. As explained earlier, neither the particularity requirement nor the rule that officers can only search where evidence might be found impose serious limits on searching the electronic haystack for the digital needle.[131]

Under this doctrinal path, courts should identify another "*Riley* moment" and rule that the plain view exception does not apply to the execution of digital search warrants. The plain view exception should be rejected in digital searches because the limitations on warrants that sufficiently limit the scope of physical searches do not limit the scope of digital searches. The factual differences between physical searches and digital searches justify a special, computer-specific approach to plain view, just as they did in *Riley* for searches incident to arrest.

Although I advocated this position somewhat tentatively before, I now conclude that it is time for courts to impose such a use restriction.[132] The trends I identified in 2005 have only accelerated.[133] Computers store more and more personal information. More and more everyday devices allow for electronic storage. The electronic haystack has become exponentially larger, making the harms of overbroad searches more severe than a decade ago. And last but not least, the Supreme Court has already adopted the basic rationale for computer-specific Fourth Amendment rules in *Riley v. California*.[134] The pieces are now in place for judicial adoption of a use restriction on nonresponsive files.

B. But Is Plain View Really the Problem, and Is Eliminating It Really the Answer?

This straightforward argument runs into a difficulty that I did not appreciate at the time of my earlier article and that I have not addressed elsewhere. Courts and commentators have uniformly assumed that the lawfulness of subsequent use depends on whether or how the plain view

---

129. *Id.* at 2480–82.

130. *See* Horton v. California, 496 U.S. 128, 139–41 (1990).

131. *See supra* notes 93–99 and accompanying text.

132. Kerr, *Digital Evidence*, *supra* note 4, at 314–17; Kerr, *Searches and Seizures*, *supra* note 9, at 582–84.

133. *See supra* notes 9–13 and accompanying text.

134. *See Riley*, 134 S. Ct. at 2482–85.

exception applies.[135] If you look closely, however, it is hardly clear that the lawfulness of using nonresponsive data in a computer search is really an issue for the plain view exception. Factual differences between one-stage physical searches and two-stage digital searches suggest that use restrictions on digital searches might turn out not to implicate the plain view doctrine at all. The plain view doctrine might not be the problem, and eliminating the plain view exception might not be the answer.

This argument may seem puzzling at first because the plain view doctrine acts as a use restriction in physical search cases. When agents execute a warrant for physical evidence, they enter the place to be searched and seize the property described in the warrant. It's a single-cycle process: search, then seizure. The plain view doctrine governs whether agents can seize nonresponsive evidence without a warrant when they are conducting the on-site search. Agents cannot use physical evidence without seizing it. Although agents could come back with a second warrant, this is difficult in the case of a physical search; the target may destroy the evidence in the meantime, and the place searched would need to be secured.[136] As a practical matter, then, the plain view doctrine imposes a use restriction by regulating when the government can seize nonresponsive property.[137]

The facts of digital searches are different, however, and that may change the role of the plain view exception in important ways. In a two-cycle digital search, the agents first take away all the computers during the physical search stage.[138] Taking away all the computers seizes all of the data that the computers contain. Next, the agents search through the already seized data and look for responsive data. If the agents come across nonresponsive data that interests them, they may want to use it. Perhaps they will use it by copying the already-seized data for use in a criminal case. Perhaps they will use it to obtain a second warrant to justify searching the computer for more related evidence. And perhaps they will simply remember what they saw and use it for new leads or to testify about their observation in court.

These factual differences raise serious questions about whether the legality of subsequent use is really a question settled by judicial embrace or by rejection of the plain view exception. First, it's unclear whether the plain view doctrine is generally implicated when the government wants to use already-seized property. Second, if the plain view exception is implicated in that context generally, it's not clear when use of observed data constitutes an

---

135. *See, e.g.*, United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1178–83 (9th Cir. 2010) (Kozinski, J., concurring); United States v. Williams, 592 F.3d 511, 521–24 (4th Cir. 2010); Kerr, *Digital Evidence*, *supra* note 4, at 314–17; Kerr, *Searches and Seizures*, *supra* note 9, at 582–84.

136. *See generally* United States v. Hill, 459 F.3d 966, 974–79 (9th Cir. 2006) (providing justification for overseizure in digital searches but requiring an explanation in the warrant affidavit).

137. *See supra* Part II.C.

138. *See supra* Part II.A.

additional seizure that the plain view exception could regulate. I'll consider each problem in turn.

The first problem is about the scope of the plain view exception. Does the doctrine ever apply to a second seizure—a seizure of property already seized? In a typical electronic search, all the contents of all the computers already have been seized from the target at the physical search stage. Assuming that using nonresponsive data is a seizure of that data, does the plain view doctrine determine whether the government can conduct a second seizure?

United States v. Jacobsen suggests that the answer may be "no."[139] In *Jacobsen*, government agents who had temporarily seized the suspect's FedEx package then destroyed (and thus permanently seized) a small amount of its contents to conduct a field test for cocaine.[140] The Court did not treat the legality of the field test's permanent seizure as a question for the plain view exception.[141] Instead, the Court asked whether the field test rendered the ongoing seizure of the contents unreasonable.[142] Following *Jacobsen*, perhaps the key question raised by the execution of computer warrants is whether use of nonresponsive data renders the ongoing seizure of the data unreasonable rather than whether the plain view exception applies to digital evidence.[143] Despite surface appearances, maybe use of nonresponsive data is not a plain view question at all.[144]

Second, assuming that the legality of the second seizure depends on whether the plain view exception applies, it's not clear when use of nonresponsive data amounts to a Fourth Amendment seizure that would be allowed or not based on judicial tweaking of the plain view exception. Courts have not yet settled what it means to "seize" data at the electronic search stage.[145] Because the plain view exception regulates seizures, it's somewhat

---

139. United States v. Jacobsen, 466 U.S. 109, 124–25 (1984).

140. *See id.* at 111–12.

141. *See id.* at 124–25.

142. *See id.*

143. This possibility is explored in detail in Part V.

144. Alternatively, perhaps the plain view exception should be understood as focusing collectively on both the initial seizure and the later act considered as a whole, rather than as its own independent exception to the warrant requirement. There is some disagreement in the Court's cases about which characterization is more accurate. *Compare* Coolidge v. New Hampshire, 403 U.S. 443, 464 (1971) (plurality opinion) (characterizing the plain view exception as an exception to the warrant requirement), *with* Texas v. Brown, 460 U.S. 730, 738–39 (1983) (arguing that "[a]t least from an analytical perspective, this description [of the plain view exception] may be somewhat inaccurate," and that the plain view exception is "perhaps better understood . . . not as an independent 'exception' to the Warrant Clause, but simply as an extension of whatever the prior justification for an officer's 'access to an object' may be"). If the plain view exception is understood as simply an extension of whatever the prior justification may be for the officer's access to the object, it's possible to see the plain view approach in this Part and the continuing seizure approach in Part V as converging into a single approach.

145. *See generally* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010) [hereinafter Kerr, *Fourth Amendment*] (discussing the different approaches courts have taken to when copying data is a seizure).

difficult to assess the impact of eliminating the plain view exception. When does the subsequent use of that exposed data revealed during the electronic search stage constitute a second seizure of that data beyond the initial seizure that occurred during the physical search stage? We don't know the answer, and yet the effect of eliminating the plain view exception may hinge on it.

Consider three possibilities. First, imagine that using the data is not an additional seizure.[146] In that case, the plain view exception would appear to be irrelevant to the use.[147] Agents could use the nonresponsive data regardless of whether the plain view exception exists because that use is not an additional seizure that the government must rely on the plain view exception to justify.[148] Under that assumption, eliminating the plain view exception for computer searches would not impose any use restriction at all.

Alternatively, imagine that actually copying data constitutes an additional seizure but that merely observing data does not.[149] In that case, ending the plain view exception for digital searches would just add a minor paperwork requirement.[150] Upon seeing the nonresponsive data, agents would simply go to a judge, report the evidence of crime that they have observed, and get a second warrant to justify additional use of the new evidence discovered. Because the files are already safely in police custody, getting a second warrant is easy whenever probable cause exists. And agents may be happy to get a second warrant: Obtaining an additional warrant triggers deferential review of the probable cause finding in a subsequent motion to suppress.[151] Under this set of assumptions, ending the plain view exception would have only a very modest effect because agents can use the nonresponsive data to get a second warrant that justifies copying it.

The third option is that all use of data observed outside the warrant constitutes an additional seizure.[152] On the plus side, this interpretation would mean that eliminating the plain view exception imposes the desired use restriction. Even obtaining a second warrant after discovering the new

---

146. *See, e.g.*, *In re* United States, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009) (holding that copying data for use is not a seizure).

147. *See, e.g.*, Horton v. California, 496 U.S. 128, 133 n.5 (1990) (noting the difference between mere observation of an item in plain view, which is not regulated by the plain view exception, and the taking away of that item, which the plain view exception regulates).

148. *See id.*

149. I have argued that this will often be the correct outcome. *See* Kerr, *Fourth Amendment*, *supra* note 145, at 711–23.

150. *See id.*

151. *See* United States v. Leon, 468 U.S. 897, 918 (1984).

152. No court has taken this position. The closest any court has come to this position is *United States v. Jefferson*, which held that agents seized data when they observed the data and took notes about what they saw. United States v. Jefferson, 571 F. Supp. 2d 696, 704 (E.D. Va. 2008). However, even the *Jefferson* court reasoned that agents did not seize anything if they merely remembered what they observed and later used it to obtain a warrant. *See id.* ("Of course, the agents are not required to erase from their memories what they saw in the documents, and if they subsequently obtain information that, coupled with what they saw, gives them probable cause to seize the documents, they may then seek a warrant to seize the documents.").

evidence would be prohibited, as the process of using the discovery of the additional information to obtain a second warrant would be an additional seizure that could no longer be justified by the plain view exception.

The downside of this interpretation is that it would be difficult to apply this definition of seizure elsewhere. No court has yet taken such a broad view of what it means to seize data, and such an interpretation might have substantial unintended consequences.[153] As I have written elsewhere, the definition of seizures in the context of digital evidence presents tricky questions and has great importance for the scope of government power.[154] Selecting a definition to achieve the instrumental goal of imposing a use restriction for warrant searches may inadvertently create even bigger problems in other contexts.

I add all of this detail not to confuse the reader—although I fear I have succeeded at that—but instead to point out that imposing a use restriction by cutting back on the plain view exception may be more complicated than it first seems. Courts might not worry about these technicalities in the course of rethinking the plain view exception. The notion that cutting back plain view acts as a use restriction is fairly intuitive in the physical context, and it is natural to assume that it applies in the same way in the digital context. But if courts are concerned about the technicalities, they may be reluctant to eliminate the digital plain view exception as a way to impose a use restriction on overseized files. They might instead want to focus on the reasonableness of the ongoing seizure. I turn to that approach next.

V. THE SECOND PATH: USE IS FORBIDDEN BECAUSE IT RENDERS THE ONGOING SEIZURE UNREASONABLE

This Part develops a better doctrinal approach to impose a use restriction on nonresponsive files in computer warrant searches. This second path resembles the plain view approach in some ways, but it ends up being more direct, less complex, and potentially narrower. Under this alternative approach, use of nonresponsive files violates the Fourth Amendment in a two-stage computer search because it renders the ongoing seizure of the nonresponsive files constitutionally unreasonable. I will call this the "ongoing seizure" approach, as it focuses on the reasonableness of the ongoing seizure of the nonresponsive data seized in a two-stage computer search.

The ongoing seizure approach focuses on the reasonableness of the continuing seizure of nonresponsive files. A valid warrant justifies the seizure and use of responsive files. On the other hand, nonresponsive files

153. *See generally* Kerr, *Fourth Amendment*, *supra* note 145, at 705–09 (discussing the definition of seizure in the context of computer data).

154. *See id.* at 705.

are seized at the physical search stage only out of investigative necessity to obtain the responsive files. Although the seizure of nonresponsive files is reasonable when needed to effectuate the search for responsive files, subsequent use of the seized nonresponsive files transforms the nature of the seizure and renders it constitutionally unreasonable.

The ongoing seizure approach imposes a use restriction much like that sought by eliminating the plain view exception.[155] At the same time, it does so more narrowly and without its potential doctrinal headaches of eliminating the plain view exception. Because the approach focuses on the facts of computer searches, it does not require a *Riley*-like announcement of a new rule just for computer searches.[156] It also does not require grappling with the technical definition of seizures raised by the plain view approach. This Part develops the ongoing seizure approach, discussing its use in the Supreme Court's decision in *United States v. Jacobsen*[157] and the Second Circuit's recently vacated panel decision in *United States v. Ganias*.[158]

A. Use of Nonresponsive Data Makes the Seizure Unreasonable

The ongoing seizure argument for use restrictions begins at the physical search stage. At the physical search stage of executing a warrant for digital evidence, the government overseizes beyond what the Fourth Amendment would normally allow.[159] The warrant traditionally provides the authorization to seize the responsive evidence described in the warrant for later use in court.[160] Courts have allowed the seizure of nonresponsive files as well as responsive files only out of necessity.[161] Responsive and nonresponsive files are commingled and difficult to separate quickly. As a result, the government can take away nonresponsive files and search the images at the government's leisure, because that is the most reasonable way to search the computer for responsive files.

Focus your attention on the reasonableness of the ongoing seizure of the nonresponsive files. Initially, before the computer is searched, the seizure is reasonable because it is necessary to effectuate the warrant. Investigative necessity also justifies officers seeing those nonresponsive files in the course of looking for the responsive files. Searching through the haystack for the needle inevitably reveals a lot of hay. That much is inevitable, as the Supreme Court has recognized.[162] Allowing the initial seizure and

155. *See supra* Part IV.

156. *See* Riley v. California, 134 S. Ct. 2473, 2488–89 (2014).

157. United States v. Jacobsen, 466 U.S. 109 (1984).

158. United States v. Ganias, 755 F.3d 125 (2d Cir. 2014), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015).

159. *See supra* note 29 and accompanying text.

160. *See Riley*, 134 S. Ct. at 2482.

161. *See supra* Part II.A and accompanying text.

162. *See* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

subsequent viewing is therefore necessary to make sure the warrant is not reduced to a dead letter.

On the other hand, the subsequent use of nonresponsive data transforms the nature and quality of the ongoing seizure of that data. Using nonresponsive data no longer effectuates the warrant. Instead, it takes advantage of the overseizure and subsequent search necessary to carry out the warrant to transform the warrant for specific evidence into the equivalent of a general warrant. In effect, allowing use of nonresponsive data effectively treats that data as if it had been included in the warrant. This eliminates the role of the particularity requirement, making the warrant the equivalent of a general warrant.[163] Subsequent use enables every computer warrant that is narrow in theory to become general in fact. Because subsequent use renders the ongoing seizure unreasonable, use of the nonresponsive files generally violates the Fourth Amendment.

From this perspective, subsequent use offends the longstanding principle of proportionality established in *Terry v. Ohio*.[164] Under *Terry*, the question is not just "whether the officer's action was justified at its inception," but also "whether it was reasonably related in scope to the circumstances which justified the interference in the first place."[165] At its inception, overseizure at the physical search stage is reasonable to effectuate the warrant.[166] But subsequently using overseized nonresponsive data is not "reasonably related in scope to the circumstances which justified the interference in the first place."[167] Expanding the scope of the seizure by allowing use of nonresponsive files has no relation whatsoever to identifying the evidence described in the warrant. It therefore renders the seizure unreasonable.

This insight suggests that imposing a use restriction is not the first "*Riley* moment" governing the execution of computer search warrants. Courts already allow the overseizure of nonresponsive files at the physical search stage.[168] A use restriction would simply counter this first *Riley* moment with a limiting principle: Agents can overseize, but they cannot receive a windfall from the overseizure. Courts should block the windfall by restoring the traditional limits on the seizure power to what was described in the warrant. They can do so by concluding that the overseizure is reasonable only when necessary to obtain the responsive data described in the warrant. Subsequent use of the nonresponsive data for reasons unrelated to carrying out the

163. *See* Kerr, *Searches and Seizures*, *supra* note 9, at 555–56.
164. *See* Terry v. Ohio, 392 U.S. 1, 20 (1968).
165. *Id.*
166. *See id.*
167. *Id.*
168. *See supra* Part II.A.

warrant renders the ongoing seizure of the nonresponsive data constitutionally unreasonable.[169]

This rule imposes a use restriction without raising the difficult questions posed by eliminating the plain view exception. Unlike altering the plain view exception, focusing on the ongoing seizure does not require identifying a second seizure.[170] It merely requires courts to identify the point at which use renders the ongoing seizure unreasonable. It also imposes a use restriction without requiring courts to take the relatively bold step of announcing a new rule just for computer searches. The ongoing seizure approach imposes a use restriction because of the two-stage nature of computer searches, rather than because "digital is different" in a more abstract sense. This context implies a clear limit on the doctrine that was uncertain under the plain view approach: The use restriction should be limited to the execution of searches using the two-stage search procedure common in computer warrant cases.

B. United States v. Jacobsen

The ongoing seizure approach is not just an academic theory: *United States v. Jacobsen* provides important precedential support for it.[171] In *Jacobsen*, agents had lawfully seized an open FedEx package that contained a substance resembling cocaine.[172] The agents conducted a field test on the substance, destroying a trace amount of cocaine.[173] At the end of the opinion, the Court considered the defendant's claim that field testing the cocaine violated the Fourth Amendment because it was an unreasonable seizure.[174]

According to *Jacobsen*, the subsequent field test was constitutionally relevant because it changed the nature of the ongoing seizure of the package.[175] "[A] seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on 'unreasonable seizures.'"[176] The field test changed the nature of the suspect's lost possession by rendering permanent the otherwise temporary loss of a trace amount of the substance.[177]

The Court then assessed the reasonableness of the field test to determine if it rendered the seizure of the destroyed substance unreasonable.[178] This

---

169. *See* Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51 (1995).
170. *See supra* Part IV.A–B.
171. *See generally* United States v. Jacobsen, 466 U.S. 109 (1984).
172. *See id.* at 111–12.
173. *See id.*
174. *See id.* at 124–25.
175. *See id.* at 125.
176. *Id.* (citing United States v. Place, 462 U.S. 696, 707–10 (1983)).
177. *See id.* at 124–25.
178. *See id.* at 125.

required "balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion."[179] The Court held the field testing constitutional because the balance of interests favored the government:

> The law enforcement interests justifying the procedure were substantial; the suspicious nature of the material made it virtually certain that the substance tested was in fact contraband. Conversely, because only a trace amount of material was involved, the loss of which appears to have gone unnoticed by respondents, and since the property had already been lawfully detained, the "seizure" could, at most, have only a *de minimis* impact on any protected property interest.[180]

It could be a different case, the Court suggested, if the government had used up more of the substance or had less of a reason to suspect that the substance was illegal.[181]

Jacobsen provides helpful precedential support for the ongoing seizure approach. *Jacobsen* analyzes a two-stage seizure that resembles the execution of a computer warrant.[182] First the entire container was temporarily seized, and then a part of its contents was used up.[183] The Court focused on how the destruction of the tested substance altered the balance of interests of the underlying seizure.[184] Applying *Jacobsen* to computer searches, use of already-seized nonresponsive files should ordinarily render the ongoing seizure of those files unreasonable in light of the balance of interests triggered by that use.

The reason goes back to the Fourth Amendment itself. On one hand, if agents can seize all of the suspect's digital property and use all that it contains, regardless of what the warrant says, the impact on the target's possessory interests is severe. The government can use and reveal the target's entire digital life, just as if the government had obtained a general warrant. On the other hand, the government's competing interest in the use of nonresponsive data is the usual interest in crime control. Although this can be a compelling interest in specific situations, in the ordinary case it is outweighed by the interest in avoiding general warrants. The Fourth Amendment itself proves the point. The Fourth Amendment leaves no

---

179. *Id.* (quoting *Place*, 462 U.S. at 703).

180. *Id.*

181. *See id.* at 126 n.28 ("An agent's arbitrary decision to take the 'white powder' he finds in a neighbor's sugar bowl, or his medicine cabinet, and subject it to a field test for cocaine, might well work an unreasonable seizure.").

182. *See id.* at 112–20.

183. *Id.* at 111–12.

184. *See id.* at 124–25.

ambiguity that general warrants are constitutionally unreasonable even if they may be useful to solve crimes.

C. What Kinds of Use Are Restricted?

If courts adopt a use restriction, the next issue is what counts as "use." The question should be what uses of nonresponsive data transform the seizure of that data in ways not "reasonably related in scope to the circumstances which justified the interference" at the outset?[185] Although I will not resolve every hypothetical here, it is worth noting the core cases as well as flagging an important gray area.

First, using nonresponsive data in court to prove the suspect's crime is obviously a core case of use. Such use treats nonresponsive data no differently than responsive data, transforming the nature of the seizure of nonresponsive data from incidental and limited to intentional and unbounded.[186] Similarly, using the discovered nonresponsive data as a basis for cause to justify an additional search or seizure for more responsive data should also count as a prohibited use.[187] As discussed earlier, if agents can use the nonresponsive data to develop probable cause to obtain a second warrant to search for additional data—either by copying it and submitting it in the warrant application or simply by describing its discovery in an affidavit—then the use restriction is largely reduced to a paperwork requirement.[188] If agents can get a second warrant so easily and expand the search accordingly, the use restriction would impose no real limit on the scope of the first warrant.[189]

The outer bounds of a use restriction are less certain. A particularly important question is whether public disclosure should count as a use that renders the ongoing seizure unreasonable. In the course of scouring through the electronic haystack for the needle described in the warrant, agents may come across nonresponsive information that is noncriminal but deeply embarrassing. Searching the suspect's computer might reveal the target's prurient interests or personal foibles. It might uncover evidence that the suspect cheated on his wife—or that his wife cheated on him. As the Supreme Court recognized in *Riley* in the context of cell phones, a computer "not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the [computer] is."[190]

---

185. Terry v. Ohio, 392 U.S. 1, 20 (1968).
186. *See supra* note 163 and accompanying text.
187. This is subject to the exigent circumstances exception discussed in Part VI.
188. *See supra* notes 149–51 and accompanying text.
189. *See supra* notes 149–51 and accompanying text.
190. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

Should public disclosure of nonresponsive information, especially with the intent to embarrass or silence a suspect, count as a prohibited use? Opinions can reasonably differ, but there is a strong case that the answer should be yes in many or most circumstances. Disclosure further infringes the person's possessory interest in his private data by making that data public and known to all. Data known to all is no longer possessed only by its owner. Pushing private data into the public domain forcibly dispossesses the target of his private data. Further, disclosure of nonresponsive data will normally not be "reasonably related in scope to the circumstances which justified the interference in the first place."[191] Disclosing nonresponsive data to the public, especially with intent to embarrass or silence, is not related to carrying out the warrant. Treating public disclosure as a use that renders the seizure unreasonable could effectively impose a nondisclosure rule for nonresponsive data in computer warrant searches akin to Federal Rule of Criminal Procedure 6(e) in the grand jury context.

D. Should Second Warrants Be Barred Even Without Use of Nonresponsive Data? The More Difficult Case of United States v. Ganias

A second important question is whether the ongoing seizure approach bars the government from obtaining a second warrant to search nonresponsive data based on probable cause developed from sources other than the nonresponsive data. For example, what if reviewing the *responsive* data shows that a broader search will reveal more evidence? Or what if investigators develop probable cause from a source other than the computer search and seek a second warrant to search the nonresponsive data a second time for newly responsive data? In that case, the nonresponsive data will not be revealed until after the government has a second warrant based on independent probable cause. Does the ongoing seizure approach bar the use with a second warrant independently obtained?

To see the problem, imagine the government obtains a warrant seeking evidence from 2013 that the suspect engaged in a specific wire fraud conspiracy. The electronic search stage reveals a responsive 2013 email in which the suspect writes to a co-conspirator: "Let's keep this scam going as long as we can; I can't believe it's been working for two years!" The responsive email provides probable cause to search the seized computer again, this time for evidence of the wire fraud conspiracy going back to 2011. Does the ongoing seizure approach ban the search under the second warrant because it allows the government to take advantage of its overseizure, or is the second search allowed because it was not based on use of the nonresponsive files?

---

191. Terry v. Ohio, 392 U.S. 1, 20 (1968).

I do not have strong views on whether the ongoing seizure approach should be limited to prohibiting use of nonresponsive files or whether it should be extended to blocking second warrants for nonresponsive data more broadly. However, it is important to note that this issue arose in the Second Circuit's recently vacated panel decision in *United States v. Ganias*, currently pending before the en banc Second Circuit.[192] A closer look at *Ganias*, and how it applied the ongoing seizure approach, is therefore in order.

Ganias is an accountant whose computers were searched twice pursuant to two different warrants.[193] First, in 2003, agents investigating Ganias's clients obtained and executed a warrant for client files stored on Ganias's computers.[194] At the physical search stage, the agents made image copies of all three of Ganias's computer hard drives on site and brought the images into government custody for later analysis.[195] By December 2004, the agents had searched the images and separated out the files that were responsive to the warrant from the files that were nonresponsive.[196]

The second search occurred in 2006.[197] By that time, agents developed probable cause to believe that Ganias himself was also guilty of crimes.[198] Ganias had by then already deleted the incriminating data that had been stored on his computers.[199] But this didn't stop the case as the agents already had a copy of his files from the 2003 search.[200] The incriminating evidence was in the set of nonresponsive files from the 2003 warrant that remained in government custody.[201] The agents sought and obtained a second warrant to search the 2003 copies of Ganias's files for Ganias's own offenses.[202] Executing the 2006 warrant on the copies in government custody revealed evidence of Ganias's crime.[203]

In the now-vacated panel opinion, the Second Circuit held that the agents violated the Fourth Amendment and that the files found during the execution of the second warrant must be suppressed.[204] The panel assumed that the agents were permitted to create mirror images of all of a suspect's files at the physical search stage in 2003.[205] Making the images seized all of those files for Fourth Amendment purposes, and the continued retention of

---

192. United States v. Ganias, 755 F.3d 125 (2d Cir. 2014), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015).
193. *Id.* at 128, 130.
194. *Id.* at 128.
195. *Id.* at 128–29.
196. *Id.* at 129.
197. *Id.* at 130.
198. *See id.* at 129.
199. *Id.* at 130.
200. *Id.*
201. *Id.* at 129.
202. *Id.* at 130.
203. *See id.*
204. *See id.* at 141.
205. *See id.* at 137.

those files made the seizure a continuing one.[206] But the Fourth Amendment gave the officers different rights with respect to responsive and nonresponsive files.[207] While the government's 2003 warrant allowed agents to permanently seize the files on Ganias's computers that were responsive to the warrant, the warrant did not give the agents unlimited authority to permanently seize and then use nonresponsive files.[208]

To keep the warrant from being "the equivalent of a general warrant," the panel held, the 2003 warrant could only grant the agents limited rights to seize the nonresponsive files at the physical search stage.[209] Although the initial overseizure was presumably permitted, the Fourth Amendment imposed limits on the retention and use of the overseized nonresponsive files: "[R]etaining the files for a prolonged period of time and then using them in a future criminal investigation" violated the Fourth Amendment.[210] Even if the government could "maintain a complete copy of the hard drive solely to authenticate evidence responsive to the original warrant," the Fourth Amendment imposed a use restriction: Any right to retain files "does not provide a basis for using the mirror image for any other purpose."[211]

The panel decision in *Ganias* shares roots with the ongoing seizure approach. *Ganias* properly focuses on the reasonableness of the ongoing seizure of the nonresponsive files.[212] In keeping with the ongoing seizure approach, *Ganias* treats the government's control of and access to nonresponsive files as distinct from its control of and access to the files described in the warrant.[213] Because the government had access to the nonresponsive files in 2006 only because it was permitted to overseize at the initial physical search stage in 2003, the Fourth Amendment placed limits on the government's ongoing seizure.[214] The basic approach mirrors the ongoing seizure approach recommended in this Article.

At the same time, the panel decision in *Ganias* adopts a particularly strong version of the ongoing seizure approach. First, *Ganias* at times suggests an affirmative requirement that the government delete nonresponsive files rather than simply not use them.[215] Such an affirmative duty is not required by the ongoing seizure approach, which could easily focus only on use rather than continued retention. An affirmative duty to delete could be difficult to implement. For example, when exactly is the duty triggered? What does it mean to "delete" data? Although the ongoing seizure

206. *See id.*
207. *See id.* at 137–38.
208. *See id.* at 138.
209. *See id.*
210. *Id.*
211. *Id.* at 139.
212. *See id.* at 136.
213. *See id.* at 137–38.
214. *See id.* at 137.
215. *See id.* at 139.

approach could be interpreted to impose an affirmative duty to delete, it need not be applied in such a far-reaching way.

Second, the panel decision in *Ganias* apparently applied the ongoing seizure approach to wall off nonresponsive data from access even with a second warrant based on independent probable cause.[216] My conclusions on this must be tentative because the precise causal relationship between the first warrant and the second warrant is not obvious from the vacated panel decision.[217] But if I am reading the panel opinion correctly, it appears that the second warrant in *Ganias* was not obtained from a review of nonresponsive electronic data overseized during the execution of the first warrant.[218]

Whether the ongoing seizure approach should apply to such facts is an open question.[219] This Article focuses primarily on a narrower version of the ongoing seizure approach, which merely bars use of nonresponsive data revealed during the execution of the first warrant. The narrow version would ensure that routine computer warrants do not become general warrants, but it could be interpreted to nonetheless allow the government to "double dip" into the nonresponsive files obtained from the first warrant with independent probable cause.[220] To be sure, courts could adopt the stronger version of the rule apparently applied by the vacated panel decision in *Ganias*, by which nonresponsive files cannot be revealed at all even with a second independent warrant. But the doctrine need not be applied so strongly to restore the basic limits of search warrants in a world of digital evidence.

VI. TERRORIST ATTACKS AND AN EXIGENT CIRCUMSTANCES EXCEPTION

Every proposal raises objections, and now I want to consider an objection I have often heard in response to my argument for use restrictions. The objection comes in the form of this question: What if the agents are searching the computer for evidence of crime in the warrant and they come across evidence of an imminent terrorist attack? Surely we don't expect the agents to sit on the evidence and let thousands of people die. Similarly, imagine officers are searching a computer and they come across nonresponsive images of the computer owner engaged in sexual crimes against a child. Officers want to take action to protect the child depicted in the pictures. Should the use restriction apply even then?

---

216. *See id.* at 137–38.

217. *See id.* at 129–30.

218. *See id.*

219. *See supra* notes 212–18 and accompanying text.

220. *See Ganias*, 755 F.3d at 129–30. As noted above, whether the probable cause for the second warrant was truly independent of the review of nonresponsive files from the first warrant is not entirely clear from the vacated decision. *Id.*

Fortunately, it should not. Courts should adopt an exigent circumstances exception to the nondisclosure rule. The rule and its exception could be stated as follows, with the exception in italics: Agents executing a computer warrant cannot use nonresponsive files revealed in the course of searching the computer for responsive files *unless the revealed nonresponsive files reveal exigent circumstances justifying that use in response to the exigency*. Under this approach, if agents are searching for tax fraud records and they come across evidence that a bomb is about to go off across town, they could use that information just as they would in any other case.[221]

The exigency exception to the nondisclosure rule should rely on the established doctrine of exigent circumstances.[222] As the Supreme Court has explained, "The need to protect or preserve life or avoid serious injury is justification for what would be otherwise illegal absent an exigency or emergency."[223] If information outside the warrant reveals need to protect or preserve life or avoid serious injury going forward, the seizure of that nonresponsive data becomes reasonable to protect life or avoid serious injury.

An exigent circumstances exception is particularly easy to justify under the ongoing seizure approach. Recall the argument for the ongoing seizure approach developed above and applied in *Jacobsen*.[224] In the ordinary case, use of nonresponsive files is unreasonable because it transforms the ongoing seizure of those files. Use of the nonresponsive files takes a reasonable seizure needed to effectuate the first warrant and changes it to an unreasonable seizure that renders the warrant the functional equivalent of a general warrant. As a consequence, later use of revealed but nonresponsive files is ordinarily not permitted.

When the nonresponsive files reveal exigent circumstances, on the other hand, the balance of interests is very different. When exigent circumstances are revealed, subsequent use advances a vital and specific interest in preventing immediate harms. The warrant is not transformed into the functional equivalent of a general warrant because the use must be narrowly tailored to the exigency. The government can only use the nonresponsive information that revealed the exigency, and it can do so only in response to the exigency. As a result, that use will be only a modest and reasonable additional intrusion into the individual's Fourth Amendment interests.

Jacobsen emphasizes the point. *Jacobsen* allowed the destruction of a small amount of suspected drugs because, in context, that additional seizure was reasonable.[225] When nonresponsive files reveal exigent circumstances,

---

221. *See supra* Part V.A–B.

222. *See, e.g.*, Missouri v. McNeely, 133 S. Ct. 1552, 1558–60 (2013) (summarizing the exigent circumstances exception).

223. Mincey v. Arizona, 437 U.S. 385, 392 (1978).

224. *See supra* Part V.A–B.

225. *See* United States v. Jacobsen, 466 U.S. 109, 125 (1984).

allowing use of those files in response to the exigency is akin to allowing the field testing of seized cocaine found reasonable in *Jacobsen*.[226] Allowing the use in that narrow context greatly advances a significant government interest at only a modest cost to Fourth Amendment interests.[227] As a result, any use restriction imposed can be subject to an exigent circumstances exception. When the government develops exigent circumstances based on a review of nonresponsive files observed in the course of executing the warrant, the agents can use those nonresponsive files to address the exigency.

VII. CONCLUSION

Two decades ago, Harold Krent argued that when the government obtains property or information through a seizure, the Fourth Amendment should impose a use restriction on the property or information seized.[228] In Krent's view, Fourth Amendment seizures are inherently limited: The government may take possession of property only so long as necessary for the public purpose that justified the seizure.[229] Krent contended that the reasonableness of any seizure should therefore factor in the subsequent use of the seized property or information.[230] Krent advocated a particularly strict kind of use restriction to ensure that seizures remain reasonable: When the government seizes information, Krent argued, the government should be required to articulate how it will use the information, and the Fourth Amendment should limit the government to that articulated use.[231]

Krent's approach goes too far by imposing a strict use restriction on information even when the government has obtained a warrant based on probable cause specifically authorizing the government to seize it. The Fourth Amendment has never been interpreted so strictly. And I do not think it should be so interpreted in the future. When a warrant application establishes probable cause to believe that information will be in a particular place, and the warrant specifically describes that information, the warrant should authorize a seizure of that information without limitation on use.

At the same time, this Article embraces Krent's thinking in a more modest and limited form. Computer technologies require overseizure and then broad government access to nonresponsive files. The government does not establish probable cause to seize that nonresponsive information; it is

---

226. *Id.* at 110.

227. *Id.*

228. *See* Krent, *supra* note 169.

229. *See id.* at 52–53.

230. *See id.* (arguing that "reasonableness of a seizure extends to the uses that law enforcement authorities make of property and information even after a lawful seizure," such that "[i]f the state can obtain the information only through means constituting a search or seizure, then use restrictions should apply, confining the governmental authorities to uses consistent with the Amendment's reasonableness requirement").

231. *See id.* at 93–98.

merely along for the ride commingled with responsive data. Although investigative necessity may give the government access to massive amounts of nonresponsive data in its possession, the absence of probable cause to seize that nonresponsive data should mean limits on its use.

To ensure that computer warrants are not executed in ways that resemble general warrants, courts should interpret the seizure power to impose use restrictions on the nonresponsive files seized and observed in the course of the government's permitted search for the responsive files. This should be the judiciary's next "*Riley* moment," triggered by the need to restore traditional Fourth Amendment limits on the warrant authority in the new world of digital searches.