VIRGINIA LAW REVIEW

ARTICLES

EX ANTE REGULATION OF COMPUTER SEARCH AND SEIZURE

Orin S. Kerr[*]

In the last decade, magistrate judges around the United States have introduced a new practice of regulating the search and seizure of computers by imposing restrictions on computer warrants. These ex ante restrictions are imposed as conditions of obtaining a warrant: Magistrate judges refuse to sign warrant applications unless the government agrees to the magistrate's limitation on how the warrant will be executed. These limitations vary from magistrate to magistrate, but they generally target four different stages of how computer warrants are executed: the on-site seizure of computers, the timing of the subsequent off-site search, the method of the off-site search, and the return of the seized computers when searches are complete.

This Article contends that ex ante restrictions on the execution of computer warrants are constitutionally unauthorized and unwise. The Fourth Amendment does not permit judges to impose limits on the execution of warrants in the name of reasonableness. When such limits are imposed, they have no legal effect. The imposition of ex ante limits on computer warrants is also harmful: Ex ante assessments of reasonableness in ex parte proceedings are highly error-prone, and they end up prohibiting reasonable practices when paired with ex post review. Al-

though ex ante restrictions may seem necessary in light of the present uncertainty of computer search and seizure law, such restrictions end up having the opposite effect. By transforming litigation of the lawfulness of a warrant's execution into litigation focusing on compliance with restrictions rather than reasonableness, ex ante restrictions prevent the development of reasonableness standards to be imposed ex post that are needed to regulate the new computer search process. Magistrate judges should refuse to impose such restrictions and should let the law develop via judicial review ex post.

INTRODUCTION

IMAGINE you are a federal magistrate judge. The FBI comes to you with a warrant application to search a suspect's home and seize his computers. You review the application and confirm that it satisfies the Fourth Amendment and the Federal Rules of Criminal Procedure.[1] The affidavit establishes probable cause, the warrant particularly describes the items to be seized, and the application is made by a federal agent to search property located in your district.[2]

But there's a catch. The Fourth Amendment regulates both the issuance of warrants and their execution.[3] Although the application satisfies the legal standards for issuing a warrant, you believe that the agents likely will violate the Fourth Amendment when they search the suspect's home, seize his computers, and then search the computers for evidence. You worry that the agents will grab more computers than they need and then look through the seized computers in an overly invasive way. You want the FBI to execute the warrant lawfully, so you consider imposing restrictions on how the warrant is executed to ensure it will be executed in a reasonable and therefore constitutional way.

The law of computer search and seizure remains undeveloped, so the ideal restrictions are uncertain. But perhaps you will sign the

---

[1] See Fed. R. Crim. P. 41 (regulating the issuance of federal search warrants).

[2] See id; see also U.S. Const. amend. IV (stating that "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").

[3] See United States v. Ramirez, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the method of execution of the warrant.") (citation omitted).

warrant only if the FBI agents agree to use a particular search protocol.[4] Or perhaps you will sign the warrant only if the government agrees to minimize the seizure of the suspect's hardware[5] or if the government agrees to waive any rights to seize any items discovered in plain view outside the warrant.[6] Whatever restriction you choose, the goal is to protect the Fourth Amendment ex ante: you can best protect the Fourth Amendment by imposing conditions when you issue the warrant on how it later will be executed.

In the last decade, many federal magistrate judges have embraced this practice.[7] Restrictions have varied widely from circuit to circuit and judge to judge, but magistrate judges generally have tried four kinds of limitations in computer warrant cases: first, conditions limiting the seizure of computer hardware from the physical place where the warrant is executed;[8] second, conditions restricting the time period before seized computers are electronically searched;[9] third, restrictions on how the computers are searched to limit access to evidence outside the warrant;[10] and fourth, conditions on when the seized hardware must be returned.[11]

Ex ante limitations on computer warrants recently received an enthusiastic endorsement by the en banc Ninth Circuit in *United States v. Comprehensive Drug Testing*,[12] a case about searching a computer file for records of steroid use in professional baseball. After announcing a series of restrictions for magistrate judges in the Ninth Circuit to impose on the execution of all computer warrants, Chief Judge Kozinski celebrated the importance of ex ante

---

[4] See infra Section I.B.

[5] See infra Section I.A.

[6] See, e.g., United States v. Comprehensive Drug Testing, 579 F.3d 989, 998, 1006 (9th Cir. 2009) (en banc) (ordering magistrate judges to require the government to waive rights to evidence discovered in plain view in computer warrant cases). See infra Section I.C.

[7] See infra Part I. For the most part, federal search warrant applications are reviewed by federal magistrate judges appointed under 28 U.S.C. § 631. This Article uses the phrase "magistrate judge" more broadly to refer to judges tasked with reviewing applications for search warrants. In particular, the phrase "magistrate judge" is used to encompass both federal and state judges.

[8] See infra Section I.A.

[9] See infra Section I.B.

[10] See infra Section I.C.

[11] See infra Section I.D.

[12] 579 F.3d 989 (9th Cir. 2009) (en banc).

restrictions on warrants to safeguard Fourth Amendment protections:

> [W]e must rely on the good sense and vigilance of our magistrate judges, who are in the front line of preserving the constitutional freedoms of our citizens while assisting the government in its legitimate efforts to prosecute criminal activity. Nothing we could say would substitute for the sound judgment that judicial officers must exercise in striking this delicate balance.[13]

The practice of conditioning computer warrants on how they are executed is a significant development in Fourth Amendment law. Many magistrate judges have embraced the practice as the best way to deal with the new dynamics of computer searches and seizures. Some scholars have agreed, envisioning such practices as important ways to limit computer searches.[14]

But is this new practice legal? And is it wise? That is, do magistrate judges have the constitutional authority to condition the issuance of warrants on how the warrants will be executed? And to the extent the legality of the practice remains open, are such restrictions wise as a matter of policy? Are such restrictions helpful tools for magistrate judges on "the front line of preserving [our] constitutional freedoms," as Judge Kozinski claims,[15] or are they misguided limitations that may backfire in practice? The scholarly literature has not yet considered these questions closely. Despite their importance, these restrictions are so new and, as magistrate judge practices, so hidden from view that legal scholarship has yet to focus on them.[16]

---

[13] Id. at 1007.

[14] See, e.g., Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, 8 Mich. Telecomm. & Tech. L. Rev. 39, 82–84 (2002) (promoting the use of search protocols for computer warrants); Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 102–14 (1994) (urging the use of search protocols to regulate computer searches and seizures ex ante).

[15] *Comprehensive Drug Testing*, 579 F.3d at 1007; Derek Haynes, Comment, Search Protocols: Establishing the Protections Mandated by the Fourth Amendment Against Unreasonable Searches and Seizures in the World of Electronic Evidence, 40 McGeorge L. Rev. 757, 772 (2009) (urging courts to require ex ante search restrictions on computer searches).

[16] The two articles and one student comment cited in note 14, supra, have recommended the adoption of ex ante restrictions, but none of the three address the lawful-

This Article shines a light on the new practices, and it then argues that ex ante regulation of computer warrants is both constitutionally unauthorized and unwise. The restrictions are unauthorized because the Fourth Amendment contemplates a narrow role for magistrate judges. Magistrate judges have no inherent power to limit how warrants are executed beyond establishing the particularity of the place to be searched and the property to be seized. When magistrate judges do impose restrictions on how a warrant is executed, those restrictions have no legal effect. The constitutionality of the search must hinge on whether the search was reasonable as judged ex post, not on whether the government complied with restrictions imposed by the issuing magistrate judge ex ante.

Ex ante regulation is also unworkable and counterproductive. Predictions of reasonableness are highly error-prone, as they are made in brief ex parte proceedings with few facts. In this setting, ex ante restrictions prohibit reasonable steps ruled out by judicial error. The scope of ex ante error will be a function of constitutional uncertainty: the more unclear the relevant legal rules, the more uncertain will be the restrictions needed to ensure reasonableness. Conversely, as the law becomes clear, predictive errors will decrease. As the law of reasonableness develops for computer searches, however, ex ante restrictions also become useless. The police will follow the rules because they know they will be imposed ex post, without a need for ex ante restrictions. From this perspective, the perceived need for ex ante restrictions is simply a response to the present legal uncertainty of computer search and seizure law.

Nor can the imposition of ex ante restrictions serve as a temporary measure until the law becomes more settled. Forward-looking regulation impairs the ability of appellate courts and the Supreme Court to develop the law of unreasonable searches and seizures in the usual case-by-case fashion. Such restrictions effectively dele-

---

ness of these restrictions other than in passing. The affirmative arguments made in favor of the lawfulness of ex ante restrictions are discussed in Section II.D, infra. In addition, I briefly addressed the wisdom of ex ante restrictions on computer search protocols in one article a few years ago, see Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 575–76 (2006). However, that argument was limited to the techniques that must be used at the electronic search stage, rather than the role of ex ante restrictions generally, and it did not address the lawfulness of such restrictions.

gate the Fourth Amendment to magistrate judges, transforming Fourth Amendment litigation away from an inquiry into reasonableness and towards an inquiry into compliance with the magistrate's commands. Search and seizure law cannot develop well or quickly in this environment. For that reason, ex ante restrictions should not be used as temporary measures until the law becomes settled. Those measures will actually prevent the law from developing.

Importantly, this is an argument about means rather than ends. The widely-accepted goal of Fourth Amendment protection is to require reasonable police practices.[17] To accomplish that goal, judges "must balance 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."[18] The judges who have imposed ex ante restrictions agree with this goal,[19] as do I. The question here is not what goal to achieve, but how to achieve it. Efforts to regulate computer search and seizure ex ante reflect the best of intentions. But whatever limitations courts impose on the execution of computer warrants, those limits should be developed and identified in ex post challenges. Magistrate judges should decline to impose such limits ex ante as conditions of issuing warrants.

The argument will be made in three parts. Part I explains the four kinds of conditions that magistrate judges have imposed on computer warrants. Part II argues that magistrate judges lack the authority to impose such restrictions under existing Fourth Amendment law. Part III contends that even if such restrictions are permitted as a matter of law, they are unwise as a matter of policy.

---

[17] See United States v. Knights, 534 U.S. 112, 118 (2001) ("The touchstone of the Fourth Amendment is reasonableness.").

[18] United States v. Place, 462 U.S. 696, 703 (1983).

[19] See, e.g., *Comprehensive Drug Testing*, 579 F.3d at 1006 (announcing ex ante search restrictions, and justifying them as "clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment").

I. FOUR TYPES OF EX ANTE CONDITIONS ON THE EXECUTION OF COMPUTER WARRANTS

The Fourth Amendment states that "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."[20] By its terms, this list is non-exclusive. It requires judicial pre-approval of probable cause and particularity, but it does not rule out other kinds of review as a condition of issuing a warrant. In the last decade, some judges have relied on this ambiguity to subject search warrants for computers to special Fourth Amendment scrutiny. This Part reviews the four kinds of limitations that courts have imposed.

To understand the new limitations, it is important to recognize how computer searches are different from traditional searches. The government executes a computer search warrant in two stages instead of one.[21] In the first stage, the physical search stage, the government enters the place to be searched and retrieves electronic storage devices that may contain the evidence sought.[22] In most cases, the government will seize the computers without searching them. In the second stage, the electronic search stage, the government conducts a forensic examination of the digital storage device for the evidence described in the warrant.[23] This process typically occurs in a government computer laboratory, and it is normally executed by trained computer specialists long after the initial physical seizure.

The precise rules governing computer search and seizure remain in their infancy, and courts today have only a tentative sense of how the Fourth Amendment applies to this new two-step process.[24] Faced with this uncertainty, some magistrate judges have begun to condition the issuance of computer warrants on how such warrants are executed. Exactly how common these practices are remains uncertain. But there have thus far been four major categories of con-

---

[20] U.S. Const. amend. IV.
[21] Orin S. Kerr, Search Warrants in an Era of Digital Evidence, 75 Miss. L.J. 85, 86 (2005) ("With computer searches, however, the one-step search process is replaced by a two-step search process.").
[22] Id. at 86–87.
[23] Id.
[24] See infra Section III.C.

ditions: a) conditions limiting the seizure of computer hardware during the physical search; b) conditions limiting the permitted timeframe of the electronic search; c) conditions on how the electronic search stage must be conducted to limit access to evidence outside the warrant; and d) conditions on when the seized hardware must be returned. This Part summarizes the cases that have imposed these four ex ante conditions.[25]

A. Conditions Limiting the Seizure of Computer Hardware at the Physical Search Stage

The first set of conditions concern seizures of electronic storage devices during the physical search stage. The problem here is a practical one. Even when agents have probable cause to believe a particular computer file is somewhere in a home, normally they cannot know which electronic storage device may contain the evidence.[26] A criminal suspect might have a few computers, several thumb drives, a few backup disks, and a large collection of writable compact disks. Agents executing a warrant cannot search all of these storage devices on the scene because it would be too time-consuming.[27] The only practical alternative is to seize most or even all of the electronic storage devices and to search them later off-site.[28]

Most courts have allowed this practice on the ground that it is the only reasonable way to execute a warrant for electronic evi-

---

[25] Some courts have announced other types of restrictions. For example, at least one magistrate judge required the government to issue status reports concerning how the electronic search was proceeding. See United States v. Voraveth, No. 07-419 DWF/AJB, 2008 WL 4287293, at *3 (D. Minn. July 1, 2008). However, the four types of restrictions discussed in this Article are the types that courts have repeatedly required.

[26] That is, they cannot know what data is stored inside each computer until the computer is searched.

[27] See United States v. Hill, 459 F.3d 966, 974–75 (9th Cir. 2006) (quoting and endorsing the district court's reasoning that "the process of searching the files at the scene can take a long time. To be certain that the medium in question does *not* contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk—a process that could take many hours and perhaps days.").

[28] See id.

dence.[29] The Ninth Circuit, however, has taken a somewhat different approach. In *United States v. Hill*,[30] the Ninth Circuit ruled that agents who wish to seize computers and search them later off-site must obtain pre-approval from the magistrate judge. "Although computer technology may in theory justify blanket seizures . . . ," Judge Fisher explained, "the government must still demonstrate to the magistrate *factually* why such a broad search and seizure authority is reasonable in the case at hand."[31] Specifically, the affidavit that establishes the basis of probable cause must also include a statement for why it is reasonable to "seize the haystack to look for the needle."[32] The statement lets the magistrate judge determine if the government's alleged need to seize physical storage devices is "reasonable" and outweighs the owner's interest in retaining his property for legitimate reasons.[33]

Notice the key analytical step underlying *Hill*. Like other circuits, the Ninth Circuit concludes that the government may over-seize at the physical stage when it is reasonable to do so. Unlike other circuits, however, the Ninth Circuit makes the reasonableness determination subject to ex ante rather than ex post review. The affidavit of probable cause doubles as an affidavit for reasonableness to seize, and the magistrate's approval of the warrant reflects the magistrate's ex ante conclusion that seizure of physical storage devices during the execution of the warrant would be constitutionally reasonable.

Some magistrate judges have imposed somewhat different requirements on seizing computer hardware during warrants. For example, in *United States v. Olander*,[34] the warrant required the gov-

---

[29] See, e.g., Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997); United States v. Schandl, 947 F.2d 462, 465–66 (11th Cir. 1991); United States v. Henson, 848 F.2d 1374, 1383–84 (6th Cir. 1988).

[30] 459 F.3d 966.

[31] Id. at 975.

[32] Id. (quotation omitted).

[33] As the Ninth Circuit put it in *Hill*:

> [T]he magistrate must be made aware of what officers are contemplating and why they are doing so. For some people, computer files are the exclusive means of managing one's life—such as maintaining a calendar of appointments or paying bills. Thus, there may be significant collateral consequences resulting from a lengthy, indiscriminate seizure of all such files.

Id. at 976 n.12.

[34] No. 06-75-HA, 2006 WL 2679542 (D. Or. Sept. 18, 2006).

ernment to examine the computer equipment during the physical search stage and "to determine whether these items can be accessed and preserved on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data in order to analyze and search it off-site."[35] Rather than assess reasonableness in the warrant application, the magistrate judge ordered the government to make that determination when the physical search was conducted as part of the condition of signing the warrant. Although this is slightly different from *Hill*, the conceptual approach is the same: the magistrate judge conditions the issuing of the warrant on a process of how the warrant will be executed.

B. Conditions Limiting the Timeframe of the Electronic Search

The second type of restriction is a limit on the timeframe of the electronic search stage. Statutory rules governing the warrant process require the government to execute physical searches within a short period after the warrant is signed.[36] The Federal Rules of Criminal Procedure have traditionally required the warrant to be executed within ten days after it is signed, for example, although that time window was recently expanded to fourteen days.[37] In contrast, no statutory rule regulates the timing of the electronic search stage for computer searches.[38] The recent amendment to the Federal Rules makes this explicit: "the time for executing the warrant" provided in the Rules "refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review."[39]

Whether the Fourth Amendment provides any limitation on the timing of the electronic search stage of a computer warrant is unclear. Courts have hinted that such limitations might exist in theory, but they have not directly imposed any such limits.[40] Faced

---

[35] Id. at *6 (quoting the warrant).

[36] At the federal level, this requirement occurs in Federal Rule of Criminal Procedure 41(e)(2)(A)(i). States have equivalent rules. See, e.g., Cal. Penal Code § 1534 (creating a ten-day rule).

[37] See Fed. R. Crim. P. 41(e)(2)(A)(i) (effective December 1, 2009).

[38] See Fed. R. Crim. P. 41(e)(2)(B) (effective December 1, 2009) ("Unless otherwise specified, the warrant authorizes a later review of the media or information.").

[39] Id.

[40] See, e.g., United States v. Syphers, 426 F.3d 461, 469 (1st Cir. 2005) (holding that "[u]nder the circumstances" a five-month delay in the search of a seized computer did

with this uncertainty, some magistrate judges have imposed their own requirements on the timeframe of electronic searches. Practices have varied widely, with individual magistrate judges imposing their own sets of limitations. Recent cases show some of the diverse approaches taken, as well as how later courts have evaluated motions to suppress based on compliance or non-compliance with these new magistrate-imposed limitations.

The first case is *United States v. Brunette*,[41] in which a magistrate judge issued a warrant to search computers on the condition that the forensic analysis of the computers had to be conducted within thirty days of the physical search. The agents executed the physical search stage five days later and seized two computers. Soon before the thirty-day window elapsed, agents applied for and received an extension from the magistrate judge giving them another thirty days to search the seized computers.[42] Agents searched one of the computers within the new thirty-day window, but they did not search the second computer until shortly after the second thirty-day period had expired.[43] Both searches revealed images of child pornography on the suspect's computers. The district court ruled that the images discovered in the renewed thirty-day window were admissible, but that the images discovered on the second computer searched after the time had expired had to be suppressed based on the government's failure "to adhere to the requirements of the search warrant and subsequent order."[44]

Brunette can be contrasted with the recent Eighth Circuit decision in *United States v. Mutschelknaus*.[45] In *Mutschelknaus*, agents obtained a warrant to search the suspect's house and seize his computers to search them for images of child pornography. The magistrate judge imposed a requirement that the electronic search of any seized computers must occur within sixty days of the initial seizure.[46] The government searched the suspect's home, seized his

---

not violate the Fourth Amendment "because there is no showing that the delay caused a lapse in probable cause, that it created prejudice to the defendant, or that federal or state officers acted in bad faith to circumvent federal requirements").

[41] 76 F. Supp. 2d 30 (D. Me. 1999), aff'd, 256 F.3d 14 (1st Cir. 2001).

[42] Id. at 42.

[43] Id.

[44] Id.

[45] 592 F.3d 826 (8th Cir. 2010).

[46] Id. at 828.

computers, and searched the computers offsite within the required sixty days. The defendant moved to suppress the evidence found on the computers on the ground that the sixty-day period was too long, and that any forensic search of the computer had to occur within the ten-day window traditionally required for warrants to be executed.[47] The Eighth Circuit disagreed, noting with approval that the agents had searched the computer within the sixty-day window approved by the magistrate judge.[48]

Whereas both *Brunette* and *Mutschelknaus* are federal decisions, the Colorado Supreme Court's opinion in *People v. Strauss*[49] shows that the same practice is occurring at the state level. Colorado state investigators obtained a warrant in 2004 to search the suspect's home for evidence stored on his computers. The warrant included an express limitation on the timing of the electronic search stage: any search of seized "computer media" had to be completed within ninety days.[50] The warrant was executed and five personal computers were seized.[51] When the suspect fled the country, however, the search of the computers became a low priority and the computers were never searched. Two years later, in 2006, the suspect reentered the country and was arrested.[52] Agents then applied for and obtained new warrants to search the computers. When agents searched the computers under the 2006 warrants, they found incriminating evidence.[53] The defendant moved to suppress the evidence on the ground that the 2006 searches violated the ninety-day rule imposed by the 2004 warrants. The Colorado Supreme Court disagreed, holding that a time limit for completing the forensic analysis from an earlier warrant did not preclude the government from reapplying and obtaining a new warrant to search the computer.[54]

---

[47] Id. Note that the warrant in this case was governed by the pre-2009 version of Rule 41. The new text of Rule 41 expressly addresses the question. See Fed. R. Crim. P. 41(e)(2)(B) (effective December 1, 2009).

[48] *Mutschelknaus*, 592 F.3d at 829–30.

[49] 180 P.3d 1027 (Colo. 2008) (en banc).

[50] Id. at 1028.

[51] Id.

[52] Id. at 1028–29.

[53] Id. at 1029.

[54] Id. at 1030–31.

In some cases, restrictions on the timing of electronic searches have become quite complex. For example, in *In re Search of the Premises Known as 1406 N. 2nd Avenue*,[55] investigators applied for a warrant to search the suspect's home for electronic evidence. The magistrate judge signed the warrant, but not before expressing significant concern that the government might search the computers at the electronic stage at any time, and that such searching might prove unconstitutional.[56] To prevent a future unconstitutional search, the judge refused to permit the government to search the seized computers until the court provided express permission.[57] Specifically, the government was ordered to report within thirty days of the physical search on what computers the government had seized and how long the government likely would need to search the seized computers.[58] The government conducted the physical search, seized one computer, and then filed its report.[59] The magistrate judge then issued an order finally permitting the government to begin searching the computer but giving the government only ninety days in which to conclude the search.[60]

The precise holdings of these various cases are less important for my purpose than the principle at work. In all of these cases, magistrate judges issued computer warrants on the condition that the government follow restrictions on the timing of the electronic search stage. These ex ante restrictions either governed the gov-

---

[55] No. 2:05-MJ-28, 2006 WL 709036 (W.D. Mich. Mar. 17, 2006).

[56] Id. at *6.

[57] Id. at *1.

[58] The order stated:

> IT IS HEREBY ORDERED that within 30 days of execution of the Search Warrant issued on August 31, 2005, a return shall be presented to the Court. The return shall identify all computer storage media, such as hard drives, CDs, DVDs, floppy disks, the variety of USB drives or thumb drives, or other forms of storage media seized, as well as all other materials seized from the residence. No forensics examination of the computer hard drive and storage media may be conducted of the materials seized until further order of this Court. At the time the return is presented to the Court, the Government shall provide an estimate of the time necessary to conduct a forensics examination of the materials seized and the computer search protocol to be utilized.

Id. at *1.

[59] Id. at *6.

[60] Id. at *7 ("The Government will be permitted to search the computer seized and the digital media evidence and is hereby ordered to conclude that search within 90 days of the date of this opinion and order.").

ernment's search process or else became the basis for motions to suppress. Reviewing courts then treated compliance with the magistrate-imposed rules as a reason to admit evidence and noncompliance as a reason to suppress evidence.

C. Conditions on How the Electronic Search Stage Must Be Conducted to Limit Access to Evidence Outside the Warrant

The third category of restrictions on warrants consists of limits on how government agents must search the computer at the electronic search stage. The problem here is that computer searches can be extraordinarily invasive.[61] Computers can store a remarkable range of different kinds of evidence and private materials on a single device, and searching that device in a comprehensive way can expose both crimes and embarrassing private information that can be admissible in court under the plain view exception.[62] To limit the amount of information outside the warrant that comes into plain view, some judges have imposed limits on how computers are searched to try to ensure searches will be as narrow as possible.

For example, in *In the Matter of the Search of: 3817 W. West End*,[63] the government applied for a warrant to search a suspect's home and seize her computers to search them for evidence of tax fraud.[64] The magistrate judge signed the warrant, but placed a condition on the warrant forbidding the government to search any seized computers until the government had proposed and the magistrate had accepted a search protocol. The government seized a Hewlett-Packard computer and a number of computer disks, and then met with the magistrate judge to discuss the search protocol.[65] The government argued that the judge lacked any authority to restrict the government's search of the seized computer, but the magistrate concluded that such a protocol was necessary to ensure that the warrant was executed in a reasonable way.[66] The judge then gave the government twenty-one days to submit a search protocol,

---

[61] Kerr, supra note 16, at 543–47.
[62] See id. at 568–71.
[63] 321 F. Supp. 2d 953 (N.D. Ill. 2004).
[64] Id.
[65] Id. at 956.
[66] Id. at 957.

with the warning that if the government did not do so it would have to return the computer unsearched.[67]

The high-water mark of judicial insistence on pre-approving search protocols is the litigation leading up to the Ninth Circuit's recent en banc decision in *United States v. Comprehensive Drug Testing.*[68] *Comprehensive Drug Testing* concerned a search pursuant to a warrant for electronic records of steroid tests taken by professional baseball players. The government obtained a warrant to search the office of the testing company for the results of ten specific players. The magistrate judge imposed a number of conditions on executing the warrant, among them that computer forensic specialists rather than the case agents had to segregate out the information described in the warrant.[69]

When the government visited the company to execute the warrant, trained computer specialists located a computer folder known as the "Tracey" directory that contained the records. The Tracey directory contained more than just the results of the ten players named in the warrant, however: it also included the test results of hundreds of other baseball players, results from participants in thirteen other sports organizations, three unrelated sporting competitions, and a business.[70] The specialists concluded that they could copy the directory without seizing the physical computers that stored the data, and they copied the file and then handed it over to the case agents. The case agents later searched the Tracey directory for the results of the ten players named in the warrant. During the course of that search, they came across the results of hundreds of other players in plain view.[71] The agents decided to use some of these test results to expand the investigation.

The Major League Baseball Players Association then filed civil suits seeking the return of the information outside the scope of the warrant so that the government could not rely on the additional information it had discovered. These challenges led to two district court orders ruling that the Players Association was entitled have the Tracey directory returned—minus the ten results named in the

---

[67] Id. at 963.
[68] 579 F.3d 989 (9th Cir. 2009) (en banc).
[69] Id. at 996.
[70] Id. at 1005.
[71] Id. at 997.

warrant—because the government had blatantly disregarded the magistrate judge's limitations on the warrant.[72] Although the warrant had required the use of case agents to identify the data described in the warrant, the case agents had actually searched the Tracey directory and had therefore discovered the additional evidence in plain view.[73] On appeal before the Ninth Circuit, Chief Judge Kozinski ruled that the government had failed to appeal this order in a timely way.[74] Although the issue was not technically before the Court of Appeals on the merits, Judge Kozinski's opinion emphasized its agreement: the government could not use the additional evidence discovered because it had discovered that evidence in violation of the search protocols.[75]

Judge Kozinski then took the opportunity to provide guidance for magistrate judges in the Ninth Circuit in computer warrant cases, with special instructions for magistrate judges to "be vigilant in observing [its] guidance."[76] According to the en banc court, magistrate judges should impose a series of conditions on computer search warrants to ensure that the government does not overreach and find evidence outside the scope of the warrant. Three of the conditions expressly concern the electronic search stage. First, magistrate judges should require the government to "waive reliance upon the plain view doctrine in digital evidence cases."[77] By conditioning the issuance of a warrant on the government's waiver, this rule would eliminate the government's incentive to execute computer warrants in a broad way that might bring evidence into plain view.[78]

Second, magistrate judges should require agents to comply with a search protocol designed to identify the items described in the warrant without also discovering other evidence.[79] The search protocol must forbid the use of tools that would discover illegality re-

---

[72] One order was entered by Judge Cooper of the United States District Court for the Central District of California; the second order was entered by Judge Mahan of the United States District Court for the District of Nevada. Id. at 993–94.

[73] Id. at 996.

[74] Id. at 994.

[75] Id. at 989, 994–97.

[76] Id. at 1006.

[77] Id.

[78] Id. at 1004–05.

[79] Id. at 999.

1258   *Virginia Law Review*   [Vol. 96:1241

lating to evidence outside the scope of the warrant.[80] Specifically, forensic software to discover particular kinds of illegality "may not be used without specific authorization in the warrant, and such permission may only be given if there is probable cause to believe that such files can be found on the electronic medium to be seized."[81]

Third, magistrate judges must require that case agents cannot conduct the electronic search themselves and must never learn of any evidence discovered outside the warrant during the electronic search.[82] The computer forensic analysis must be performed either by computer specialists who are not on the case or a non-government third party hired to conduct the analysis.[83] In either event, the case agents with primary responsibility for bringing criminal charges must be walled off from any evidence outside the warrant's scope.[84]

At this stage, focus less on the specific rules than the conceptual framework the rules reflect. The basic idea is that judges can control the reasonableness of searches ex ante by imposing restrictions on how warrants are executed. The restrictions require the government to comply with the magistrate judge's required way of executing the warrant. The magistrate withholds approval of the search, even though the government has established particularity and probable cause, based on the magistrate's prediction of what searches will be reasonable.

D. Conditions On When Seized Hardware Must Be Returned

The final set of restrictions are those ordering the return of seized computers. Recall that the government often needs to seize computer hardware and search it off-site to find the evidence described in the warrant.[85] The permitted over-seizure can result in a suspect's property remaining in government possession indefinitely. Although a computer owner can file a Rule 41 motion for return of property, the government otherwise has no freestanding

---

[80] Id.
[81] Id.
[82] Id. at 1000.
[83] Id.
[84] Id.
[85] See supra notes 21–23 and accompanying text.

obligation to return property seized under a proper warrant.[86] Some magistrate judges have responded to this by imposing restrictions ordering the government to return seized computers at a particular time as a condition of issuing the warrant.

Such restrictions have occurred most often in investigations involving commercial enterprises. For example, in *In re Searches and Seizures*,[87] the government obtained a warrant to search the office of a real estate company for evidence of tax fraud and other crimes. The warrant included the condition that the government return the computers within ninety days of the initial seizure absent an additional order from the magistrate judge.[88] Similarly, in *United States v. Maali*,[89] the government obtained warrants to search the computers of a company suspected of involvement in immigration offenses. The warrant specified that after seizing the company's computers, "the government will return the computers promptly after retrieving and storing the information contained therein, which period will not exceed ten days."[90]

The en banc Ninth Circuit in *Comprehensive Drug Testing* took a more far-reaching approach.[91] Instead of imposing a time restriction in business cases, the Ninth Circuit ordered magistrate judges to impose limits on the return of computers and destruction of any copies for all computer warrants. *Comprehensive Drug Testing* announced a specific set of rules to follow when the electronic search is complete:

> Absent further judicial authorization, any remaining copies [of data] must be destroyed or, at least so long as they may be lawfully possessed by the party from whom they were seized, returned along with the actual physical medium that may have been seized (such as a hard drive or computer). The government may not retain copies of such returned data, unless it obtains

---

[86] That is, the warrant authorizes the search and seizure but does not require property to be returned. The onus is on the person whose property was seized to file a motion under Rule 41. See Fed. R. Crim. P. 41(g).

[87] Nos. 08-SW-0361 DAD, 08-SW-0362 DAD, 08-SW-0363-DAD, 08-SW-0364 DAD, 2008 WL 5411772 (E.D. Cal. Dec. 19, 2008).

[88] Id. at *2.

[89] 346 F. Supp. 2d 1226 (M.D. Fla. 2004).

[90] Id. at 1245.

[91] 579 F.3d 989, 1000–01 (9th Cir. 2009) (en banc).

specific judicial authorization to do so. Also, within a time speci-
fied in the warrant, which should be as soon as practicable, the
government must provide the issuing officer with a return dis-
closing precisely what data it has obtained as a consequence of
the search, and what data it has returned to the party from whom
it was seized. The return must include a sworn certificate that the
government has destroyed or returned all copies of data that it is
not entitled to keep. If the government believes it is entitled to
retain data as to which no probable cause was shown in the origi-
nal warrant, it may seek a new warrant or justify the warrantless
seizure by some means other than plain view.[92]

Again, the details of these rules are not important for the pur-
poses of this Article. Rather, the key is the approach. The warrants
require the government to follow the magistrate's restrictions on
how to execute the warrant—in this case, when to return the seized
equipment or destroy copies made. As with the other limitations,
the magistrate judges are taking an active role in the execution of
the warrant. They are not merely issuing the warrant, but rather
are regulating the entire search and seizure process. And they are
doing so using ex ante restrictions entered as conditions of execut-
ing the searches for electronic evidence.

II. THE SUPREME COURT AND THE ROLE OF MAGISTRATE JUDGES IN ISSUING WARRANTS

Does the Fourth Amendment law allow judges to impose restric-
tions on the execution of computer warrants to ensure that they are
executed in a reasonable way? This Part reviews the Supreme
Court case law on the role of magistrate judges in the execution of
search warrants. These cases are rarely addressed in Fourth
Amendment scholarship. That scholarship tends to focus on sexy
questions like what is a search, or how specific exceptions should
or should not apply.[93] In contrast, there is very little scholarship on

---

[92] Id.

[93] By way of example, a Westlaw query for articles that mentioned the phrases "rea-
sonable expectation of privacy" and "fourth amendment" in the JLR database on
March 3, 2010 yielded 4608 hits. A query the same day for the phrase "magistrate
judge" within the same sentence as "authority" and that also used the phrase "fourth
amendment" yielded only 128 hits.

the role of magistrate judges in issuing warrants.[94]

A review of that case law indicates that existing Fourth Amendment doctrine contemplates a surprisingly narrow role for magistrate judges. Magistrate judges are required to assess probable cause and particularity, and to comply with other rules imposed under state or federal statutory law. But magistrate judges appear to have no inherent power to limit how warrants are executed in the name of constitutional reasonableness. The reasonableness of executing warrants must be determined by judicial review ex post rather than ex ante. When a magistrate does impose an ex ante restriction on a warrant, the restriction has no legal effect. The constitutionality of the search hinges on whether the search was reasonable as judged ex post, not whether the government complied with restrictions imposed by the magistrate ex ante.

Finally, the narrow role suggested in the Supreme Court's decisions is reflected in statutory warrant authorities. Warrants are regulated by statutory law in addition to the Fourth Amendment. The federal search warrant statute and most analogous state statutes use language that denies judges the power to reject warrant applications based on how they are executed. The statutory authorities state that judges "must" issue warrants when probable cause has been satisfied. The combination of Fourth Amendment case law and statutory text strongly suggests that magistrate judges are acting outside their proper authority in imposing ex ante restrictions, and that such restrictions are unenforceable and have no legal effect.

A. Lo-Ji Sales v. New York *and the Requirement Not to Act as an "Adjunct Law Enforcement Officer"*

The Supreme Court's leading case on the limited role of magistrate judges in the execution of a warrant is probably *Lo-Ji Sales v.*

---

[94] Perhaps the most notable example is Abraham S. Goldstein, The Search Warrant, the Magistrate, and Judicial Review, 62 N.Y.U. L. Rev. 1173 (1987), an article on the good faith exception to the Fourth Amendment for defective warrants. Even this article only mentions the role of the magistrate's discretion in passing. See id. at 1196 (noting that "[t]he few cases on [whether a magistrate judge can decline to issue warrants based on fears that it will be executed unconstitutionally] hold that a judge has a 'ministerial' duty to issue a warrant after 'probable cause' has been established").

New York.[95] *Lo-Ji Sales* presents the extreme case of a magistrate judge controlling the execution of the warrant by participating in the search.[96] Although it involves an extreme case, the Supreme Court's harsh rejection of the judge's creative role in executing the warrant suggests a narrow role for magistrate judges.

Lo-Ji Sales involved a search of a bookstore for obscene materials. A police officer had purchased two obscene films from an adult bookstore, and he approached a local magistrate for a warrant to search the store.[97] The officer wanted to seize obscene films beyond the two that he already purchased and viewed, but he did not know which of the other films satisfied the constitutional test for obscenity. He therefore asked the magistrate to help him execute the search. Under the officer's proposal, the magistrate would accompany the officers to the store with a warrant that initially listed only the two known films as items that that the government could seize.[98] The magistrate judge would review the additional materials himself onsite, and then tell the officers which films they could seize based on the magistrate's judgment about what was obscene. The magistrate agreed, and he came to the search site and pre-approved which films counted as obscene and therefore were seizable. After the magistrate approved the seizure of a particular film, he would add the name of the film to the warrant and the government would seize the film.[99]

The Supreme Court unanimously rejected this unusual arrangement.[100] The open-ended warrant did not specify what could be seized, and the magistrate's on-site control hurt rather than helped matters. Specifically, the magistrate's participation in the execution of the warrant violated the Fourth Amendment's requirement of a neutral and detached magistrate.[101] According to the Court, the magistrate had "telescope[d] the processes of the application for a

---

[95] 442 U.S. 319 (1979).

[96] Id. at 322.

[97] Id. at 321.

[98] Id.

[99] Id. at 321–22.

[100] Id. at 328.

[101] Id. at 326–28; cf. Coolidge v. New Hampshire, 403 U.S. 443, 450–51 (1971) (holding that the Fourth Amendment does not permit a warrant to be issued by the Attorney General).

warrant, the issuance of the warrant, and its execution."[102] As a result, the magistrate "allowed himself to become a member, if not the leader, of the search party which was essentially a police operation."[103] There was no bad faith on the magistrate's part, the Court made clear: the magistrate was simply trying to make sure that a neutral officer made the judgment as to how to execute the warrant.[104] But by combining the issuance and execution of the warrant, the magistrate "was not acting as a judicial officer but as an adjunct law enforcement officer."[105]

Lo-Ji Sales significantly undercuts the rationale of ex ante limitations on computer warrants. Like the judge in *Lo-Ji Sales*, a magistrate judge who tries to control the execution of the warrant to ensure it is reasonable "telescope[s] the processes of the application for a warrant, the issuance of the warrant, and its execution."[106] Ex ante restrictions turn the warrant application process into something much more than a check on probable cause and particularity. The restrictions try to regulate the entire process all at once. It's true that ex ante restrictions do not require the judge to be present when the warrant is executed, unlike in *Lo-Ji Sales*. But they do impose a virtual presence: the judge ensures that his own judgment as to how to execute the warrant will control the execution of the search much like the magistrate controlled the execution of the search in *Lo-Ji Sales*.

To be clear, the procedure rejected in *Lo-Ji Sales* differs from the imposition of ex ante search restrictions on computer warrants in a critical respect. The judge in *Lo-Ji Sales* was making impromptu judgments on what to seize, not how to search. But that difference cuts against the lawfulness of ex ante search restrictions, not in its favor. Determining what items the police have probable cause to seize is a core traditional function of magistrate judges reviewing warrant applications.[107] A warrant is a judicial order allowing the government to enter the place to be searched to seize the

---

[102] *Lo-Ji Sales*, 442 U.S. at 328.

[103] Id. at 327.

[104] Id. at 326–27.

[105] Id. at 327.

[106] Id. at 328.

[107] See U.S. Const. amend. IV (stating that "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").

items the judge has allowed to be seized. In contrast, how a warrant should be executed is traditionally a question for the police rather than the judge issuing the warrant.

B. Dalia v. United States *and the Standard of Ex Post Review*

The second case on the role of judicial review in the execution of warrants is *Dalia v. United States*.[108] In *Dalia*, the FBI obtained a warrant under the Wiretap Act to use a surveillance device to listen in on the office conversations of a suspect named Dalia, who was believed to be engaged in a conspiracy to steal property.[109] The warrant permitted agents to use the bug, but it did not say anything about how the government was supposed to install it.[110] In the case of a traditional physical search, of course, such an extra step would be unnecessary. Government agents execute a search and seizure all at once by entering the property and removing the information described. Bugging is different. Like a computer search, bugging a private space occurs in two stages instead of one. The Government first enters the property to install the device, and it later turns on the device to listen in on the conversations. The FBI wiretap order in *Dalia* did not mention the first stage, however.[111] By its terms, it only authorized the second stage.

The FBI executed the warrant by covertly entering Dalia's office at midnight and spending three hours installing a listening device in the ceiling.[112] They later turned on the listening device pursuant to the warrant. When the warrant expired, the agents re-entered the office covertly and removed the bug.[113] The government tried to prove Dalia's crimes using the recordings of Dalia's private conversations. Dalia responded by filing a motion to suppress based on the warrant's failure to authorize the physical search.[114] Dalia made a range of arguments, two of which are important here. First, Dalia argued that that the Fourth Amendment required the warrant to say that it would be executed by means of a covert entry. Second,

---

[108] 441 U.S. 238 (1979).
[109] Id. at 241–42.
[110] Id.
[111] Id. at 241–42, 245.
[112] Id. at 245.
[113] Id.
[114] Id. at 245–46.

Dalia argued that that electronic surveillance warrants were "unique" and required special treatment because they involved two different sets of interests: the invasion of the physical space to install the device and the invasion of privacy to listen in on the conversations.[115]

The Supreme Court disagreed. First, the Court rejected the notion that the warrant was defective because it did not explain how it could be executed. "Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that . . . warrants . . . must include a specification of the precise manner in which they are to be executed,"[116] the Court explained. "On the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant—subject of course to the general Fourth Amendment protection 'against unreasonable searches and seizures.'"[117]

Second, the Court rejected the notion that warrants for electronic surveillance were unique because their execution required two distinct stages, the entry and the listening, each of which raised different interests.[118] According to the Court, "This view of the Warrant Clause parses too finely the interests protected by the Fourth Amendment."[119]

> Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant. For example, police executing an arrest warrant commonly find it necessary to enter the suspect's home in order to take him into custody, and they thereby impinge on both privacy and freedom of movement. . . . Similarly, officers executing search warrants on occasion must damage property in order to perform their duty. . . .
>
> It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set

---

[115] Id. at 257.
[116] Id.
[117] Id.
[118] Id. at 257–58.
[119] Id. at 257.

forth precisely the procedures to be followed by the executing of-
ficers. Such an interpretation is unnecessary, as we have held—
and the Government concedes—that the manner in which a war-
rant is executed is subject to later judicial review as to its reason-
ableness.[120]

Dalia has direct relevance for computer searches because the
case for ex ante restrictions on computer warrants resembles the
claim for special treatment of bugging warrants. In both cases, the
warrants are executed in two stages. Physical entry comes first, fol-
lowed by a search of the space second. In both cases, the break-
down of the warrant process into two stages raises special privacy
issues. And yet *Dalia* rejected the argument that the two-stage
warrant requires ex ante approval of how the warrant was to be
executed. Instead, the Court concluded that the execution of bug-
ging warrants should be judged using the same ex post review for
reasonableness that occurs with traditional warrants.[121]

To be fair, *Dalia*'s usefulness is limited by the nature of the de-
fendant's claim in that case: Dalia argued that a restriction on the
method of executing the warrant was *required*, not that it was per-
mitted. Further, Dalia was seeking only a very bare-bones state-
ment as to how the physical search would be conducted: as Justice
Brennan explained in his dissent, a blanket statement that covert
entry was permitted would have been sufficient.[122] In contrast, the
question here is whether ex ante restrictions as to the method of
execution are permitted, and the restrictions at issue can be quite
detailed. At the same time, the Court's rejection of the idea that
two-stage warrants raise special concerns, and its emphasis on the
general practice of having ex post rather than ex ante review,
seems to undercut the rationale of ex ante search restrictions on
computer warrants.

---

[120] Id. at 257–58 (citations omitted). Justice Brennan dissented from this section,
joined by Justice Stewart. See id. at 259–62 (Brennan, J., dissenting).

[121] Id. at 257–58.

[122] Id. at 261 (Brennan, J., dissenting).

C. United States v. Grubbs *and the Plain Text of the Fourth Amendment*

The third important case on the role of magistrate judges in issuing warrants is *United States v. Grubbs*.[123] *Grubbs* reviewed a Ninth Circuit decision on the requirements of anticipatory warrants.[124] Anticipatory warrants are warrants based on probable cause to believe that evidence will be in a particular place in the future even though the evidence is not there when the warrant is signed.[125] Anticipatory warrants are premised on the idea that at a future time, some event will happen that will bring the evidence to the place to be searched; at that time the warrant can be executed and the place searched.[126] Such warrants are used mostly in narcotics cases to allow searches when drug deliveries are accepted.[127]

The Ninth Circuit decision under review in *Grubbs* invalidated an anticipatory warrant because it did not contain a particular description of the triggering condition—that is, the event that would happen to bring the evidence to the place to be searched.[128] Under Ninth Circuit precedent, anticipatory warrants were required to have a particular description of the triggering condition in order to limit the government's discretion on when the warrant could be executed.[129] That case law instructed magistrate judges to be "particularly vigilant in ensuring that the opportunities for exercising unfettered discretion are eliminated . . . [by] set[ting] conditions governing an anticipatory warrant that are 'explicit, clear, and narrowly drawn so as to avoid misunderstanding or manipulation by government agents.'"[130]

The Supreme Court reversed in an opinion by Justice Scalia.[131] Justice Scalia reasoned that the plain text of the Fourth Amendment did not require anything beyond a particular description of the place to be searched and the property to be seized: "The lan-

---

[123] 547 U.S. 90 (2006).

[124] 377 F.3d 1072 (9th Cir. 2004).

[125] 2 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 3.7(c), at 398 (4th ed. 2004).

[126] *Grubbs*, 547 U.S. at 94.

[127] LaFave, supra note 125, § 3.7(c), at 399.

[128] *Grubbs*, 377 F.3d at 1080.

[129] Id. at 1078 (citing cases).

[130] United States v. Ricciardelli, 998 F.2d 8, 12 (1st Cir. 1993) (quotations omitted).

[131] *Grubbs*, 547 U.S. at 99.

guage of the Fourth Amendment . . . does not include the conditions precedent to execution of the warrant."[132] Scalia also rejected the argument that a particular description of the triggering condition was needed to limit the government's discretion in executing the warrant. "That principle is not to be found in the Constitution,"[133] Scalia intoned. "The Fourth Amendment does not require that the warrant set forth the magistrate's basis for finding probable cause, even though probable cause is the quintessential 'precondition to the valid exercise of executive power.' Much less does it require description of a triggering condition."[134]

The relevance of *Grubbs* lies in the similarity between the rationale for ex ante restrictions on anticipatory warrants and the rationale for ex ante restrictions on computer warrants. The Ninth Circuit had required its magistrate judges to pre-approve the triggering condition to limit the government's discretion in how it executed the warrant: the purpose was to "ensur[e] that the opportunities for exercising unfettered discretion [we]re eliminated."[135] This rationale had no takers on the Supreme Court. The Court adhered instead to the plain text of the Fourth Amendment, which requires only a particular description of the place to be searched and the items to be seized.[136] According to the Court, the extra requirement of preapproval of the triggering condition in the warrant itself was not permitted. The requirement simply was "not to be found in the Constitution."[137]

D. Richards v. Wisconsin *and the Legal Effect of Ex Ante Restrictions*

The combination of *Lo-Ji Sales*, *Dalia*, and *Grubbs* suggests that magistrate judges should not impose ex ante restrictions on warrants to ensure they are executed in a reasonable way. Some judges appear to be doing it anyway, however, which raises an important question: What are the legal consequences if the government breaches a magistrate's ex ante restriction?

---

[132] Id. at 98.
[133] Id.
[134] Id.
[135] *Ricciardelli*, 998 F.2d at 12.
[136] *Grubbs*, 547 U.S. at 98–99.
[137] Id. at 98.

This issue arose in *Richards v. Wisconsin*,[138] and the Court's decision indicates that the answer is "none." *Richards* concerned the Fourth Amendment's knock-and-announce rule, a rule that agents executing a warrant normally must knock and announce their presence as police officers before entering a home.[139] Under an exception to the rule, agents can dispense with the rule if they have a reasonable suspicion to believe that knocking and announcing their presence would be dangerous, futile, or inhibit the investigation.[140]

In *Richards*, agents sought a warrant to search a hotel room for drugs based on suspicion that Richards was selling drugs from inside it. The agents asked the judge to sign a warrant permitting them to execute it without first knocking and announcing their presence.[141] The magistrate judge found probable cause and signed the warrant, but he expressly rejected the request to dispense with the knock-and-announce requirement by crossing out that part of the warrant.[142] When the agents executed the warrant, however, they did not announce their presence.[143] The discovery of cocaine and cash in the hotel room led to charges, and the defendant moved to suppress on the ground that the agents had violated the knock-and-announce rule.[144] Further, the agents had expressly violated the magistrate judge's will: the judge had declined to let the officers dispense with the requirement but they had done so anyway.

---

[138] 520 U.S. 385, 395 (1997).

[139] See generally Wilson v. Arkansas, 514 U.S. 927, 930 (1995) (holding that the common-law knock-and-announce rule is part of the Fourth Amendment reasonableness inquiry).

[140] *Richards*, 520 U.S. at 394.

[141] Id. at 388 ("The police requested a warrant that would have given advance authorization for a 'no-knock' entry into the motel room, but the Magistrate explicitly deleted those portions of the warrant.").

[142] Id.

[143] The agents executed the warrant by going to the hotel room and having an officer pose as a maintenance man who needed to enter. Richards cracked open the door in response to the knock at the door, but he saw a uniformed officer behind the "maintenance man" and he quickly slammed it shut. The officers then kicked down the door and forcibly entered and found cocaine inside. Id. at 388–89.

[144] Note that this claim was made over a decade before the Supreme Court held that the exclusionary rule does not apply to knock and announce violations. Hudson v. Michigan, 547 U. S. 586, 599 (2006).

The Supreme Court disagreed in a unanimous opinion by Justice Stevens.[145] According to Justice Stevens, the magistrate's refusal to allow a no-knock warrant had no effect.[146] The refusal did "not alter the reasonableness of the officers' decision" to execute the warrant without knocking and announcing.[147] The reasonableness of entering without announcing their presence "must be evaluated as of the time they entered the motel room," Justice Stevens reasoned, based on the "actual circumstances" the officers confronted.[148] The issuing magistrate could not know these circumstances ex ante, as he "could not have anticipated in every particular the circumstances that would confront the officers when they arrived at Richards' motel room."[149] Although the officers did not have evidence to execute a no-knock warrant when the warrant was obtained, at least "in the judgment of the Magistrate,"[150] what mattered was whether they had that evidence at the moment they entered. "[A] magistrate's decision not to authorize a no-knock entry should not be interpreted to remove the officers' authority to exercise independent judgment concerning the wisdom of a no-knock entry at the time the warrant is being executed."[151]

Viewed in isolation, individual cases like *Lo-Ji Sales*, *Dalia*, *Grubbs*, and *Richards* do not definitively rule out the lawfulness of ex ante restrictions on the execution of computer warrants. Taken together, however, these four cases undercut every aspect of the lawfulness of such restrictions. *Lo-Ji Sales* requires magistrates to take a hands-off approach to executing warrants;[152] *Dalia* rejects the notion that two-stage warrants raise special concerns that justify a deviation from the normal rule;[153] *Grubbs* rejects limitations designed to ensure the reasonableness of searches;[154] and *Richards* indicates that such restrictions, where imposed, have no legal ef-

---

[145] *Richards*, 520 U.S. at 395–96.
[146] Id. at 395.
[147] Id.
[148] Id. at 395–96.
[149] Id. at 396.
[150] Id. at 395.
[151] Id. at 396 n.7.
[152] 442 U.S. 319, 328 (1979).
[153] 441 U. S. 238, 257–58 (1979).
[154] 547 U.S. 90, 98 (2006).

fect.[155] All four cases emphasize that the reasonableness of a search pursuant to a warrant must be assessed ex post rather than ex ante. Taken together, these four cases point to the conclusion that the Fourth Amendment does not permit ex ante restrictions on the execution of computer warrants. Where such restrictions are imposed, they have no legal effect.

E. Statutory Warrant Rules

The limited role of magistrate judges in issuing warrants is echoed by the mandatory language used in many search warrant statutes. Whereas the Fourth Amendment provides a general framework, warrant statutes explain the procedural details of who can obtain the warrant, how it can be obtained, when it can be executed, and how a return on the warrant must be filed.[156] The text of these different statutes varies, but many of them, including the federal version, make clear that judges must issue warrants when investigators apply for a warrant and establish probable cause. The lack of discretion to deny a warrant is consistent with the view that judges do not have the authority to condition issuance of a warrant on its execution.

At the federal level, Rule 41(d)(1) of the Federal Rules of Criminal Procedure states unambiguously that "[a]fter receiving an affidavit or other information, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—*must* issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device."[157] The word in Rule 41 is not "may," "can," or even "should." Rather, the word is "must." The federal rule governing arrest warrants uses similar language,[158] and the Third Circuit has emphasized that this lan-

---

[155] 520 U.S. at 395–96.

[156] This was not always the case. Before 1917, for example, federal judges did not have explicit statutory authority to issue warrants. Congress passed a statute in 1917 codifying the common law process for obtaining search warrants. See Act of June 15, 1917, ch. 30, 40 Stat. 228 (repealed 1948). Section 3 of the Espionage Act provided, "A search warrant can not [sic] be issued but upon probable cause, supported by affidavit, naming or describing the person and particularly describing the property and the place to be searched." Id.

[157] Fed. R. Crim. P. 41(d)(1) (emphasis added).

[158] See Fed R. Crim. P. 4(a) ("If the complaint or one or more affidavits filed with the complaint establish probable cause to believe that an offense has been committed

guage is mandatory, leaving the court with no discretion to "refuse to issue an arrest warrant once probable cause for its issuance has been shown."[159] The similarity between the search warrant statute and arrest warrant statute suggests that the same principle holds for arrest warrants: The court has no discretion to refuse to issue an arrest warrant after probable cause has been established.

Many state statutes employ similar language. For example, New Jersey's warrant statute states that "[i]f the issuing magistrate is satisfied of the existence of the grounds of the application, or that there is probable cause to believe their existence, he must issue a search warrant . . . ."[160] California's statute uses nearly identical language: "If the magistrate is thereupon satisfied of the existence of the grounds of the application, or that there is probable cause to believe their existence, he or she must issue a search warrant. . . ."[161] Ohio's law states that "[i]f the judge is satisfied that probable cause for the search exists, he shall issue a warrant identifying the property and naming or describing the person or place to be searched."[162] Oregon's statute expresses the same idea in a different way: If the legal requirements for a warrant are met, the warrant statute provides, "the judge shall issue a search warrant . . . . If the judge does not so find, the judge shall deny the application."[163] Colorado's rule states that "[i]f the judge is satisfied that grounds for the application exist or that there is probable cause to believe that such grounds exist, he shall issue a search warrant . . . ."[164]

Not all states use this mandatory language. Some state statutes roughly or exactly track the language of the Fourth Amendment and therefore leave the question open.[165] But the mandatory language used in many or even most state warrant provisions echoes

---

and that the defendant committed it, the judge must issue an arrest warrant to an officer authorized to execute it.").

[159] United States v. Santtini, 963 F.2d 585, 596 (3d Cir. 1992).
[160] N.J. Stat. Ann. § 33:1-57 (West 1994).
[161] Cal. Penal Code § 1528(a) (West 2000).
[162] Ohio Rev. Code Ann. § 2933.23 (West 2006).
[163] Or. Rev. Stat. Ann. § 133.555(2) (West 2003).
[164] Colo. Rev. Stat. § 16-3-304(1) (2009).
[165] For example, Pennsylvania's statute states that "[n]o search warrant shall issue but upon probable cause," 42 Pa. Stat. Ann. § 203 (West 2007). Like the Fourth Amendment itself, this text does not expressly take a position on whether the magistrate has authority to impose additional requirements.

the limited role of magistrate judges observed in Supreme Court precedent. The statutes generally say that the judge "must" or "shall" issue the warrant if probable cause has been established. The statutes cannot establish that magistrate judges lack the power as a matter of constitutional law, of course: Legislatures can forbid what the Fourth Amendment does not. But the statutes appear to reflect a shared understanding that judges lack the discretion to deny warrant applications when the judges fear that such warrants may be executed in an unconstitutional way.

F. A Response to Counterarguments

One court and one scholar have offered different perspectives, and it is helpful to address them here. In one case, *In the Matter of the Search of: 3817 W. West End*,[166] the government argued to Magistrate Judge Sidney Schenkier that he had no power to impose ex ante restrictions in the form of a search protocol. Judge Schenkier disagreed on several grounds, but his primary argument was that ex ante restrictions such as search protocols are a part of the particularity requirement.[167] The ex ante restrictions ensure that the search will be narrow, which is an important reason why the Fourth Amendment requires a particular description of the items to be seized.[168] According to Judge Schenkier, "When there are concerns about the particularity of a given search, as is the case here, it is both sensible and constitutionally required to address those concerns at the front end of the process, and to resolve them in a way that avoids the later suppression of evidence."[169]

Whatever the merits of this argument when it was made in 2004, it seems foreclosed by *United States v. Grubbs*, handed down two years later.[170] Recall that the lower court in *Grubbs* had required a particularized description of the triggering conditions for anticipatory warrants: the idea was that by controlling the timing that the warrant was executed, courts could take away the discretion of the police to execute the warrant at an unreasonable time in further-

---

[166] 321 F. Supp. 2d 953, 957 (N.D. Ill. 2004).

[167] Id. at 961–62. An additional ground was the fact that other computer warrant cases and authorities had recommended such steps. Id. at 962.

[168] Id. at 962.

[169] Id.

[170] *Grubbs* was decided in March 2006. 547 U.S. 90 (2006).

ance of particularity principles.[171] Justice Scalia's opinion in *Grubbs* specifically rejected the notion that there are general particularity concerns in the Fourth Amendment in addition to the place to be searched and things to be seized:

> The Fourth Amendment . . . does not set forth some general "particularity requirement." It specifies only two matters that must be "particularly describ[ed]" in the warrant: "the place to be searched" and "the persons or things to be seized."[172]

The particularity of the triggering condition simply did not fit into this framework: "The language of the Fourth Amendment is . . . decisive here; its particularity requirement does not include the conditions precedent to execution of the warrant."[173]

The same goes for search protocols and other ex ante restrictions. It is true that they try to address some of the same policy concerns as the particularity requirement. Both are aimed, at a high level of abstraction, at limiting the scope of the privacy invasion. But a particular description of how the search must be executed is neither a description of the place to be searched nor a description of the items to be seized. Instead, it is just like the particular description of the triggering condition rejected in *Grubb*s: it is a limitation on how the warrant must be executed.

On the scholarly side, Susan Brenner and Barbara Frederiksen have argued that magistrate judges have the power to impose ex ante restrictions on computer warrants.[174] Brenner and Frederiksen claim that this power "derives from Rule 41 of the Federal Rules of Criminal Procedure and from the court's inherent power to issue a warrant whenever the requirements of the Fourth Amendment are met."[175] Brenner and Frederiksen wrote their argument before *Grubbs*, however, and they root much of their argument in the pre-*Grubbs* caselaw that *Grubbs* rejected.[176]

The remainder of Brenner and Frederiksen's argument is based on the recognition that the statutory regulation of federal warrants

---

[171] *Grubbs*, 377 F.3d 1072, 1079 (9th Cir. 2004).

[172] *Grubbs*, 547 U.S. at 97.

[173] Id. at 98.

[174] Brenner & Frederiksen, supra note 14, at 82.

[175] Id. at 83 (citation omitted).

[176] Id. at 83 nn.127–29.

did not occur until 1917, and yet federal courts issued warrants long before then.[177] The problem is that the power to issue a warrant absent statutory authorization does not imply the power to deny warrants unless the government complies with restrictions beyond probable cause and particularity. As *Grubbs* shows, courts are not free to add requirements to Fourth Amendment warrants based on concerns about how warrants are executed.[178] This is particularly clear in light of the language in Rule 41, which Brenner and Fredericksen do not confront.[179] As noted above, Rule 41 states that judges "must issue" the warrant when probable cause is established.[180] This mandatory language seems to rule out an inherent power to deny a warrant application based on concerns that the warrant might be executed in an unconstitutional way.

The strongest case for Brenner & Fredericksen's position derives from language in the Advisory Committee Notes for recent changes to Rule 41. In 2009, Rule 41 was amended to account for some of the specific issues raised by computer search and seizure. One of the 2009 changes clarified that the Rule's restrictions on when a search must occur—presently within fourteen days after the warrant is signed—refer to the physical search stage rather than the electronic search stage.[181] The Advisory Committee Notes to this change offered the following commentary:

---

[177] Id. at 83 n.128 (quoting United States v. Villegas, 899 F.2d 1324, 1334 (2d Cir. 1990)).

[178] See also United States v. Payner, 447 U.S. 727, 733 (1980) (holding that courts cannot use the federal supervisory power as a supplement to Fourth Amendment protections).

[179] In fairness, the clear phrase "must issue" did not appear until the 2002 revisions to Rule 41, which were undertaken for stylistic reasons to clarify the rule's meaning. See Fed. R. Crim. P. 41 advisory committee's note (2002 amendments) ("The language of Rule 41 has been amended as part of the general restyling of the Criminal Rules to make them more easily understood and to make style and terminology consistent throughout the rules. These changes are intended to be stylistic only . . . ."). Before the 2002 amendments, the Rule stated that "[i]f the federal magistrate judge or state judge is satisfied that grounds for the application exist or that there is probable cause to believe that they exist, that magistrate judge or state judge *shall issue* a warrant . . . ." Fed. R. Crim. P. 41(c)(1) (2000) (emphasis added). Although both the phrases "shall issue" and "must issue" are reasonably clear, the existing phrase "must issue" is emphatic and unambiguous.

[180] Fed. R. Crim. P. 41(d)(1).

[181] See supra notes 37–39.

> The rule does not prevent a judge from imposing a deadline
> for the return of the storage media or access to the electroni-
> cally stored information at the time the warrant is issued.
> However, to arbitrarily set a presumptive time period for the
> return could result in frequent petitions to the court for addi-
> tional time.[182]

The significance of this language is unclear. On one hand, it ap-
pears to reflect an understanding that at least some kinds of ex
ante restrictions on computer warrants are permitted. On the other
hand, Committee Notes to amendments are not the Rule itself: at
best the Notes reflect assumptions among the members of the Ad-
visory Committee rather than the requirements of the Rule. Those
assumptions understandably reflect the prevailing state of practice
at the time the Amendments were made. As a result, this language
in the Notes may indicate only that members of the Advisory
Committee in 2009 assumed that the ex ante restrictions found in
the case law are lawful, rather than a reasoned decision that such
restrictions are permitted.

Even if the language in the Advisory Committee Notes can be
construed as establishing that ex ante restrictions are permitted
under Rule 41, the remedies scheme for violating such restrictions
is a separate question. Provisions in Rule 41 have no independent
constitutional significance.[183] As a result, Rule 41 violations gener-
ally do not lead to Fourth Amendment remedies such as suppres-
sion unless the violations happen to trigger violations of the Fourth
Amendment independently of the warrant restriction.[184] Even if

---

[182] See Fed. R. Crim. P. 41 advisory committee's note.

[183] See, e.g., United States v. Johnson, 660 F.2d 749, 753 (9th Cir. 1981) (stating that
"[o]nly a 'fundamental' violation of Rule 41 requires automatic suppression, and a
violation is 'fundamental' only where it, in effect, renders the search unconstitutional
under traditional fourth amendment standards") (internal quotation marks omitted).

[184] See United States v. Hornick, 815 F.2d 1156, 1158 (7th Cir. 1987) (noting that "it
is difficult to anticipate any violation of Rule 41, short of a defect that also offends the
Warrant Clause of the fourth amendment, that would call for suppression"). There is
some authority indicating that a prejudicial or deliberate violation of technical aspects
of Rule 41 can lead to suppression independently of any Fourth Amendment viola-
tion. See, e.g., United States v. Luk, 859 F.2d 667, 673 (9th Cir. 1988). However, it ap-
pears that this standard applies to violations of requirements written into the text of
Rule 41 rather than restrictions written into warrants by magistrate judges. Even if

Rule 41 permits ex ante restrictions, the admissibility of evidence rests on the reasonableness of the search rather than compliance with ex ante restrictions.

III. THE NORMATIVE CASE AGAINST EX ANTE RESTRICTIONS FOR COMPUTER WARRANTS

Even assuming that ex ante restrictions are lawful, are they good policy? Proponents of ex ante restrictions, both in the judiciary and the academy, reason that ex ante restrictions are a powerful tool for protecting Fourth Amendment interests. As Judge Kozinski argued in *United States v. Comprehensive Drug Testing*, magistrate judges are on the front lines of the Fourth Amendment:

> [W]e must rely on the good sense and vigilance of our magistrate judges, who are in the front line of preserving the constitutional freedoms of our citizens while assisting the government in its legitimate efforts to prosecute criminal activity. Nothing we could say would substitute for the sound judgment that judicial officers must exercise in striking this delicate balance.[185]

Is Judge Kozinski right? Are ex ante restrictions on the execution of computer warrants a sensible way to balance privacy and security interests in the new world of computer searches and seizures?

The proper answer is "no." Ex ante restrictions are unworkable and unwise for two core reasons. First, the combination of error-prone ex ante judicial review and more accurate ex post judicial review will result in systematic constitutional error. Instead of requiring reasonableness, ex ante review will result in reasonable steps being prohibited by judicial error. The likelihood of error will be a function of constitutional uncertainty. The more unclear the relevant legal rules, the more uncertain will be the restrictions needed to ensure reasonableness. However, as the law of reasonableness becomes clear, ex ante restrictions also become useless: the police will follow the rules because they know they will be imposed ex post, without a need for ex ante restrictions. From this perspective,

---

Rule 41 implicitly permits ex ante restrictions, it does not require them. Cf. Richards v. Wisconsin, 520 U.S. 385, 395 (1997) (discussed supra Section II.D).

[185] United States v. Comprehensive Drug Testing, 579 F.3d 989, 1007 (9th Cir. 2009) (en banc).

the perceived need for ex ante restrictions is merely a response to present legal uncertainty.

Of course, it is better to prohibit unreasonable searches ex ante than invalidate them ex post while the law remains uncertain. Perhaps this carves out a role for ex ante restrictions, just as a place-holder until the law becomes settled? Again, the answer is "no." The difficulty is that ex ante restrictions impair the ability of appellate courts and the Supreme Court to develop the law of unreasonable searches and seizures in the usual case-by-case fashion. Assuming ex ante restrictions are not null and void, they transform Fourth Amendment litigation away from an inquiry into reasonableness and towards an inquiry into compliance with the magistrate's commands. Search and seizure law cannot develop in this environment. For that reason, ex ante restrictions cannot be temporary measures used until the law becomes settled. Ironically, those measures will actually prevent the law from being settled.

The final Section explains why the Fourth Amendment's ex ante restrictions of probable cause and particularity do not implicate the same difficulties. Ex ante assessments of probable cause and particularity primarily measure the government's interest in making the search: they reflect the common law judgment that probable cause and particularity are enough justification for a search. In contrast, ex ante search restrictions found in recent computer search and seizure cases apply a modern cost-benefit concept of reasonableness that requires a tailoring between the government's interest and the privacy invasion. That difference is critical. It explains why traditional ex ante restrictions on probable cause and particularity effectively limit searches while the new restrictions imposed for computer searches do not.

A. The Reasonableness Framework for Searches with Warrants

The Fourth Amendment prohibits unreasonable searches and seizures, and requires that searches pursuant to warrants be executed in a reasonable way. The modern framework of reasonableness requires a cost-benefit balance: the court "balance[s] 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."[186] This standard requires courts to "slosh [their] way through the factbound morass," as Justice Scalia memorably described the reasonableness standard in *Scott v. Harris*.[187] For each set of facts, the courts articulate what the officers can do and cannot do as they execute the warrant.

In the case of executing a warrant, for example, officers cannot execute the warrant in "flagrant disregard" of its terms.[188] In addition, officers normally cannot bring media reporters along to film the execution of the warrant.[189] They must knock and announce the government presence before entering the place to be searched unless it would be dangerous, futile, or inhibit the investigation.[190] They cannot search individuals located at the place to be searched without special cause.[191] They cannot look in places too small to fit the evidence described in the warrant.[192] They cannot seize evidence outside the scope of the warrant unless its incriminating nature is immediately apparent, amounting to probable cause that the additional item is evidence of a crime.[193]

On the other hand, officers can conduct a comprehensive search at the site, opening all containers and locked boxes and invading everywhere evidence could be located.[194] Officers can destroy or damage property incident to the invasive search.[195] They can detain individuals found at the location searched to control them and en-

---

[186] United States v. Place, 462 U. S. 696, 703 (1983).

[187] 550 U.S. 372, 383 (2007).

[188] United States v. Shi Yan Liu, 239 F.3d 138, 140 (2d Cir. 2000) ("Government agents flagrantly disregard the terms of a warrant so that wholesale suppression is required only when (1) they effect a widespread seizure of items that were not within the scope of the warrant, and (2) do not act in good faith.") (citations omitted).

[189] Wilson v. Layne, 526 U.S. 603, 614 (1999).

[190] Richards v. Wisconsin, 520 U.S. 385, 394 (1997).

[191] Ybarra v. Illinois, 444 U.S. 85, 91 (1979) (finding that a warrant to search a bar did not permit the search of patrons for evidence described in the warrant).

[192] United States v. Ross, 456 U.S. 798, 820–21 (1982).

[193] Arizona v. Hicks, 480 U.S. 321, 326–27 (1987).

[194] See *Ross*, 456 U.S. at 821 ("[A] warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found. A warrant to open a footlocker to search for marihuana would also authorize the opening of packages found inside.").

[195] See United States v. Ramirez, 523 U.S. 65, 71–72 (1998) (prohibiting only "[e]xcessive or unnecessary destruction of property").

sure they do not destroy evidence or pose a threat to the police.[196] They can seize evidence found outside the scope of the warrant if the incriminating nature of that evidence is immediately apparent.[197] All of these steps are reasonable as a matter of law when the government executes a warrant to search a physical space.

All of these rules, both the limitations and the authorizations, have been announced on a case-by-case basis in ex post review. Ex post review provides the standard method for developing the case law of the reasonableness of searches executed pursuant to warrants. The government executes the warrant first. Then, when charges are filed, a defendant will move to suppress the evidence discovered.[198] The court will hold a hearing about precisely how the warrant was executed, and will then issue an opinion as to whether the method of execution was reasonable.

When repeated over time, this type of litigation leads to rules and standards governing the reasonableness of how warrants are executed. In some cases, the courts will announce a relatively bright-line rule. For example, in *Wilson v. Layne*, the Supreme Court announced that the government may not bring along the media or third parties when they execute a warrant if those parties are not used to aid in the execution of the warrant.[199] In other cases, courts hand down a more malleable standard, such as the knock-and-announce rule that is waived if there is reasonable suspicion to believe compliance would be futile.[200] All of these rules and standards are handed down in ex post litigation, when the court has the trial and appellate record and can then announce whether that procedure was reasonable or unreasonable in light of all the facts.

---

[196] See Muehler v. Mena, 544 U.S. 93, 98–99 (2005) (permitting temporary handcuffing of individuals on site of execution of a warrant).

[197] *Hicks*, 480 U.S. at 326–27.

[198] Alternatively, and more rarely, a plaintiff who was victimized by a search will bring a lawsuit alleging that the search was unreasonable.

[199] 526 U.S. 603, 614 (1999) ("We hold that it is a violation of the Fourth Amendment for police to bring members of the media or other third parties into a home during the execution of a warrant when the presence of the third parties in the home was not in aid of the execution of the warrant.").

[200] See Richards v. Wisconsin, 520 U.S. 385, 394 (1997) ("In order to justify a 'no-knock' entry, the police must have a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence.").

Now consider the effect of ex ante restrictions on warrants. When magistrate judges add ex ante restrictions, they effectively create two different sources of rules regulating a warrant's execution. If the ex ante restrictions are not just dead letter and are actually intended to govern the search, the government will be regulated by two sources of law. The first source is the set of Fourth Amendment rules and standards developed and announced ex post that can be enforced in a motion to suppress or a civil action. The second source is the set of restrictions imposed ex ante by the issuing magistrate judge. The government must follow both sets of rules.

B. Why Ex Ante Restrictions Introduce Constitutional Error

Ex ante restrictions tend to introduce constitutional errors in this environment. To be sure, such restrictions stem from the best of intentions: they reflect a good-faith effort to identify what will be constitutionally reasonable.[201] However, ex ante predictions of reasonableness will be more error prone than ex post assessments for two major reasons. First, ex ante restrictions require courts to "slosh [their] way through the factbound morass of reasonableness"[202] without actual facts. Second, ex ante restrictions are imposed in ex parte hearings without legal briefing or a hearing. Both reasons suggest that ex ante restrictions often will inaccurately gauge the reasonableness of how warrants are executed.

The major difficulty with ex ante restrictions is that the reasonableness of executing a warrant is highly factbound, and judges trying to impose ex ante restrictions generally will not know the facts needed to make an accurate judgment of reasonableness. Granted, magistrate judges might have a ballpark sense of the facts, from which they might derive a sense of what practices are ideal. For example, they might think that it is unreasonable to seize all of a suspect's home computers if on-site review is possible. Alternatively, they might think it is unreasonable to conduct a search for image files if the warrant only seeks data not likely to be stored as an image. They might think it is unreasonable to keep a suspect's computer for a very long period of time without searching it. All of

---

[201] See supra text accompanying notes 4–14.
[202] Scott v. Harris, 550 U.S. 372, 383 (2007) (quotation omitted).

these senses will be based on a rough concept of how the competing interests of law enforcement and privacy play out in typical computer searches and seizures.

At the same time, these ballpark senses of reasonableness can never improve past very rough approximation. A magistrate judge cannot get a sense of the exigencies that will unfold at each stage of the search process. The reasonableness of searching on-site will not be known until the agents arrive and determine how many computers are present, what operating systems they use, and how much memory they store. The needed time window before the government searches the seized computer depends on how much the government can prioritize that case over other cases, given existing forensic expertise and resources, as well as which agency happens to be working that case.[203] The reasonableness of different search protocols depends on the operating systems, an analyst's expertise in forensics, which forensics programs the government has in its possession, what kind of evidence the government is searching for, and whether the suspect has taken any steps to hide it.[204] Finally, the reasonableness of retaining seized computers that have already been searched depends on whether the government might need the original computer as evidence or whether it ends up containing contraband that should not be returned and is subject to civil forfeiture.[205]

The magistrate presented with an application for a warrant simply cannot know these things. Judges are smart people, but they do not have crystal balls that let them predict the number and type of computers a suspect may have, the law enforcement priority of that particular case, the forensic expertise and toolkit of the examiner who will work on that case, whether the suspect has tried to hide evidence, and if so, how well, and what evidence or contraband the seized computers may contain. Magistrate judges can make ballpark guesses about these questions based on vague senses of what happens in typical cases. But even assuming they take the time to

---

[203] This is true because the forensic search process is highly resource-intensive and also costly. Agencies have a range of expertise and competing priorities and the time needed to search a computer will reflect such realities.

[204] See Kerr, supra note 16, at 575–76.

[205] See generally 18 U.S.C. §§ 2253–54 (2006) (providing for the civil forfeiture of property used in the possession and distribution of child pornography).

learn about the latest in law enforcement resources and the computer forensics process—enough to know about typical cases—they cannot do more than come up with general rules that they think are useful for those typical cases.

The errors of ex ante restrictions are particularly likely to occur because warrant applications are ex parte. The investigators go to the judge with an affidavit and a proposed warrant.[206] The judge reads over the materials submitted. The judge can modify the warrant, but his primary decision is whether to sign or reject it. The entire process takes a matter of minutes from start to finish. No hearing occurs. There is no testimony beyond the affidavit in most cases, and the affidavit usually contains only standard language about computer searches.[207] A prosecutor may be present, but need not be. Obviously, no representative of the suspect is present to offer witnesses or argument.

In that setting, judges are particularly poorly equipped to assess reasonableness. The most they can develop is a standard set of ex ante restrictions that they use in *all* computer warrants, perhaps one shared with other magistrate judges in their district. More careful scrutiny is both impractical and unlikely. The ability of a magistrate judge to assess reasonableness in that setting is a far cry from her ability to rule on reasonableness in an ex post hearing, in which agents and experts can take the stand and counsel for the defendant can cross-examine the agent, offer his own witnesses, submit written briefs, and present oral argument.

Some magistrate judges have implicitly recognized their factual and legal disadvantage by allowing decisions to be made later or allowing the government to petition for an amendment of restrictions. For example, in *United States v. Brunette*,[208] the government was given thirty days to search seized computers but was then given a thirty-day extension upon request. In *In the Matter of the Search of: 3817 W. West End*,[209] the warrant allowed the government to execute the physical search and then submit a proposed

---

[206] See Fed. R. Crim. P. 41.

[207] See, e.g., U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations app. F at 241–48 (3d ed. 2009) (offering sample standard language for a computer warrant affidavit).

[208] 76 F. Supp. 2d 30, 42 (D. Me. 1999), aff'd, 256 F.3d 14 (1st Cir. 2001).

[209] 321 F. Supp. 2d 953, 954 (N.D. Ill. 2004).

search protocol for the electronic search. In *United States v. Olander*,[210] the warrant contained a condition formally delegating the task of reasonableness to the officers. The warrant formally required the government to examine the computer equipment during the physical search stage and then make a reasonableness judgment as to whether the computers needed to be seized.[211] All of these conditions implicitly recognized that the magistrate judge could not accurately gauge reasonableness ex ante.

At the same time, all of the ex ante restrictions will necessarily be poor proxies for an ex post review of reasonableness. Instead of substituting for ex post review of reasonableness, ex ante restrictions supplement those restrictions. Ex ante limitations force the government to follow two sources of law: the reasonableness of executing the warrant imposed by reviewing courts ex post, and the restrictions imposed by the magistrate judge ex ante. If the ex ante restrictions happen to be modest, or are drafted in a way that ensures that they are always less than or equal to the restrictions of reasonableness ex post, then such restrictions will merely replicate the ex post reasonableness determinations. But every time an ex ante restriction goes beyond ex post reasonableness, the restrictions will end up prohibiting the government from doing that which is constitutionally *reasonable*. The limitations will be unreasonable limitations caused by judicial error.

C. Ex Ante Restrictions in the Face of Technological Change and Legal Uncertainty

Once the limitations of warrant restrictions are clear, such restrictions only seem desirable when the law of reasonableness has not yet been developed by appellate courts.[212] Recall Judge Kozinski's view that magistrate judges are "in the front line of preserving the constitutional freedoms of our citizens while assisting the gov-

---

[210] No. 65-75-HA, 2006 WL 2679542, at *6 (D. Or. Sept. 18, 2006).

[211] Id.

[212] Alternatively, individual magistrate judges may wish Fourth Amendment rules to be more restrictive than they are under existing appellate doctrine. Surely this is a matter for appellate courts rather than magistrate judges, however. See United States v. Payner, 447 U.S. 727, 737 (1980) (holding that courts cannot use the federal supervisory power as a supplement to Fourth Amendment protections).

ernment in its legitimate efforts to prosecute criminal activity."[213] Magistrate judges are indeed on the front lines in an important sense: they see all the warrants that the government seeks. In contrast, district court judges generally only see warrants when they are challenged in litigation, and appellate judges only see warrants in the relatively rare cases when warrants are challenged on appeal. Further, statutes that regulate the execution of warrants generally require agents to inventory what was seized and file that inventory with the magistrate judges that issued the warrants.[214] This means that magistrate judges are the first ones to see changes in the kinds of warrants that the government is seeking. They are the first ones to recognize when technological change has altered the process of executing warrants.

This is particularly important in cases involving computer warrants because the Justice Department's own internal guidance on obtaining computer warrants has in the past recommended that the affidavit should inform the magistrate judge as to how the warrant will be executed.[215] The Justice Department's 2001 guidance recommended that the affidavit inform the magistrate judge about the need to seize hardware and use specific search protocols in searching the seized computer.[216] As the author of this guidance when it was published in 2001, I can report that the original purpose of providing this information was to blunt ex post challenges to computer warrants. Under the law of most circuits, evidence within the scope of a warrant is not subject to suppression unless a warrant is executed in "flagrant disregard" of its terms.[217] If a magistrate

---

[213] United States v. Comprehensive Drug Testing, 579 F.3d 989, 1007 (9th Cir. 2009) (en banc).

[214] See, e.g., Fed. R. Crim. P. 41(f)(1)(D).

[215] U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 236 (1st ed. 2001) ("The affidavit should also contain a careful explanation of the agents' search strategy . . . . The affidavit should explain the agents' approach [to executing the warrant] in sufficient detail that the explanation provides a useful guide for the search team and any reviewing court.").

[216] Id. I authored this manual in its original form published in 2001 under the guidance of other lawyers in the Computer Crime and Intellectual Property Section at the Department of Justice.

[217] United States v. Shi Yan Liu, 239 F.3d 138, 140 (2d Cir. 2000) ("Government agents flagrantly disregard the terms of a warrant so that wholesale suppression is required only when (1) they effect a widespread seizure of items that were not within

knows how the warrant will be executed and signs the warrant, then surely an officer who follows the course of action described in the affidavit has not flagrantly disregarded its terms. That was the idea, at least.

Ironically, the procedure designed to blunt defense challenges may have inadvertently encouraged additional ex ante restrictions. Informing magistrate judges of the shift in practices that occur with computer searches ensured that they were among the first judges to recognize the new two-step process of executing computer warrants. At present, how the standard of reasonableness governs computer searches is a major question mark. The different courts to have considered these issues have only reached a small number of the issues raised, and those courts have often divided as to the answers.[218] The very first computer-specific amendments to Federal Rule of Criminal Procedure 41 went into effect just last year, and for the first time they offer some narrow guidance on computer searches.[219] But magistrate judges wondering what Fourth Amendment law governs the execution of warrants presently have few answers: the law of reasonableness that they would normally expect to be imposed ex post has not yet been developed.

Ex ante restrictions likely appear desirable to some magistrate judges only because the law of reasonableness has not yet been fully developed. To see this, imagine the law thirty years from now, when many of the issues presently open presumably will be well-settled. Imagine, just to fill in the blanks, that the Supreme Court has decided a range of cases on the reasonableness of warrants, all imposed in ex post decisions, and come up with the following rules: 1) the government is always free to seize computers for an off-site search, but it must return a copy of the seized data within ten days; 2) seized computers must be searched in a reasonable time, with "reasonable" meaning a default of nine days, with the government able to petition for more time if needed; 3) there is no required

---

the scope of the warrant, and (2) do not act in good faith.") (citations and quotations omitted).

[218] Compare United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010) (rejecting subjective approach to plain view of computer files), with United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (adopting subjective approach to plain view of computer files).

[219] See supra notes 36–39.

protocol for searching computers, but any evidence discovered outside the scope of the warrant cannot be used and must be destroyed; and 4) seized computers must be returned when the search is complete unless charges have formally been filed.

Now imagine you are a federal magistrate judge and the FBI comes to you with a warrant to search and seize computers. At this point, ex ante restrictions are no longer needed. The law of reasonableness is now clear, so you do not have to guess what would be reasonable. More importantly, there is no reason to impose restrictions ex ante. The Supreme Court rules announced ex post do it for you. When the Supreme Court hands down a rule on the reasonableness of executing a warrant, that rule essentially becomes an unwritten condition of all future warrants. Government agents will know they must follow the rule when they execute the warrant not because it is written into the warrant but because it is written into the United States Reports.

D. Ex Ante Restrictions Prevent the Development of Ex Post Reasonableness

Ex ante restrictions only have an arguable role when appellate courts have not yet determined the rules of reasonableness. Does this mean that magistrate judges should continue to impose ex ante restrictions until the appellate courts and Supreme Court settle the rules? After all, it is much better for an unconstitutional search not to occur than for the Constitution to be violated and a court to then announce the violation. Should magistrate judges continue to impose such restrictions until that law of computer search and seizure becomes clear?

The proper answer is "no." The reason is that ex ante restrictions themselves impair the ability of appellate courts and the Supreme Court to develop the law of reasonableness. Ex ante restrictions effectively delegate the Fourth Amendment to magistrate judges, transforming Fourth Amendment litigation away from an inquiry into reasonableness and towards an inquiry into compliance with the magistrate's commands. Search and seizure law cannot develop in this environment. Ex ante restrictions effectively deny courts an opportunity to announce the law in a de novo fashion. For that reason, ex ante restrictions cannot be temporary measures used until the law becomes settled. Ironically, those

measures designed to further constitutional reasonableness will actually prevent the law of reasonableness from developing.

To understand why ex ante restrictions inhibit the development of legal standards of reasonableness, we need to return to how Fourth Amendment law develops. The trial judge holds a hearing, makes factual findings, and hands down a ruling. That ruling can then be appealed, which can then lead to an appellate decision. The appellate decision reviews the facts under a clearly erroneous standard and the law de novo,[220] meaning that the appellate court reviews the lawfulness of the search and seizure without any deference to the magistrate judge who signed the warrant or the trial judge who made an initial legal ruling.[221] When an appellate court reaches the merits of the lawfulness of the government conduct, the court renders a de novo ruling on reasonableness based on factual claims as asserted by the plaintiff or, more rarely, from a jury verdict. Rulings based on de novo legal conclusions can then be appealed up to the U.S. Supreme Court, which can hand down a decision articulating how the reasonableness of the Fourth Amendment applies to a particular set of facts.

This process does not work well with ex ante restrictions. When a magistrate imposes ex ante restrictions on a search warrant, and those restrictions are understood to be binding, the ex ante restrictions naturally become the focal point of litigation on the lawfulness of the warrant's execution. The restrictions provide a clear standard. Defense challenges to the lawfulness of the warrant's execution will point first to violations of that standard.[222] Challenges will focus not on the reasonableness of the warrant execution, but rather the compliance or lack of compliance with the magistrate judge's restrictions. The cases on ex ante restrictions confirm the dynamic. In case after case, the litigation concerns whether the government complied with the magistrate's limitation,

---

[220] See, e.g., United States v. White, 593 F.3d 1199, 1202 (11th Cir. 2010).

[221] In the case of a civil action, the process is somewhat similar, although the doctrine of qualified immunity can often stop litigation without a ruling on the merits. See Pearson v. Callahan, 129 S.Ct. 808, 818 (2009) (allowing judges to decide qualified immunity issues without addressing the merits using "their sound discretion").

[222] See supra Sections I.A. and I.B.

not whether the government's conduct was constitutionally reasonable.[223]

This focus interferes with the usual process of Fourth Amendment rulemaking by effectively delegating the governing legal standard to individual magistrate judges. It denies appellate judges their usual means of establishing reasonableness by ensuring that appellate judges are not asked to review the reasonableness of the government's conduct. On appeal, the defendant will argue that the government should lose because law enforcement violated the ex ante restrictions: the focus becomes the ex ante restrictions, not constitutional reasonableness. Appellate courts will be in the position of deciding whether the government complied with the restrictions and the significance of those violations. The constitutional reasonableness of the government's conduct not only won't be decided, it may not even be briefed.

This dynamic arguably explains the extremely unusual Ninth Circuit en banc decision in *Comprehensive Drug Testing*.[224] The Ninth Circuit's decision is a true blockbuster. If it stays on the books, it will revolutionize computer search and seizure law. But it is also one of the oddest decisions in the Federal Reporter. That oddness results in part from the fact that the litigation over the warrant executing in *Comprehensive Drug Testing* was almost exclusively about whether the FBI violated the ex ante restrictions, not whether its conduct was reasonable.[225] After agreeing that the government had violated the restrictions, and that the violations justified a ruling for the plaintiffs, Chief Judge Kozinski then announced a comprehensive set of new ex ante restrictions for magistrate judges to impose.[226]

---

[223] See supra notes 41–91 and accompanying text.

It may seem surprising to some that defense lawyers would not routinely assert both claims. But from a strategic perspective, I think it is sensible for defense counsel to challenge only the violations of ex ante restrictions. In most circuits, the reasonableness of warrant execution under existing precedents is measured under the highly deferential "flagrant disregard" standard. This standard is extremely difficult for defense counsel to satisfy. In contrast, it will often be quite clear that the government violated an ex ante restriction. In that setting, arguing both positions will only draw attention to difference between the ex ante restriction and the prevailing reasonableness standard.

[224] 579 F.3d 989 (9th Cir. 2009) (en banc).

[225] Id.

[226] Id. at 1006–07.

The *Comprehensive Drug Testing* court did not say whether the rules handed down were based on the Fourth Amendment, the federal supervisory power, or something else. This likely resulted from the dynamic of the lower court litigation: because the litigation focused entirely on compliance with the ex ante restrictions, the Ninth Circuit's task was largely addressed to assessing compliance. The ex ante restrictions took on a life of their own. Instead of using the facts of the case to analyze the reasonableness of the government's searches and seizures, resulting in a rule or standard of reasonableness imposed ex post, the en banc Ninth Circuit simply announced new restrictions for magistrate judges to impose ex ante.[227]

E. The Special Case of Probable Cause and Particularity

At this point the reader may have an objection: isn't requiring ex ante review of probable cause and particularity a core function of the Fourth Amendment? As Justice Jackson famously stated in *United States v. Johnson*:

> The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.[228]

If ex ante assessments of probable cause and particularity are such an important part of the Fourth Amendment, why can't such restrictions limit the execution of the warrant as well?

The reason is that ex ante assessment of probable cause and particularity serves a different function than ex ante assessment of

---

[227] The Department of Justice has petitioned for rehearing before the full en banc court and indicated that it will petition for certiorari if the petition for rehearing is denied, so the future of the *Comprehensive Drug Testing* litigation remains uncertain. See Brief for Plaintiff-Appellant, United States v. Comprehensive Drug Testing, Nos. 05-10067, 05-15006, 06-55354 (9th Cir. Nov. 23, 2009), available at http://volokh.com/wp/wp-content/uploads/2009/11/CDT-Full-En-Banc-Response.pdf.

[228] 333 U.S. 10, 13–14 (1948).

how a search should be executed. Ex ante assessment of probable cause and particularity only measures the government's interest in making the search. It is a one-sided check: it asks only whether the government has established a fair probability that evidence of crime or contraband are located in the home, business, or other place to be searched.[229] Admittedly, the check provides only a modestly accurate assessment of the government's interest: the most obvious difficulty, introduced by Justice Brennan's opinion in *Warden v. Hayden*,[230] is that evidence of *any crime* can suffice. As a result, the government can get a warrant for more serious and less serious crimes alike.[231] At the same time, the basic structural role of requiring ex ante review of probable cause and particularity is to ensure that the government has a substantial interest in solving crime or recovering contraband.

As William Stuntz has observed, ex ante review of probable cause and particularity ensures that the assessment of the government's interest is unbiased by the eventual discovery of evidence or contraband in the place to be searched.[232] By requiring the government to go on the record and testify about its interest before the search occurs, and by requiring a neutral magistrate to confirm that interest under a veil of ignorance as to whether the government's suspicions are valid, determinations of probable cause and particularity before the search occurs ensures a relatively unbiased assessment of government interest.[233]

By contrast, ex ante restrictions on how a warrant is executed address a different question. Reasonableness requires a balance. The court must balance "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 intru-

---

[229] Illinois v. Gates, 462 U.S. 213 (1983) (defining probable cause in the case of a search warrant as "a fair probability that contraband or evidence of a crime will be found in a particular place").

[230] 387 U.S. 294, 304–07 (1967).

[231] That is, the Fourth Amendment permits warrants based on probable cause to believe a crime has been committed, but does not inquire as to the seriousness or desirability of the law defining the offense.

[232] William J. Stuntz, Warrants and Fourth Amendment Remedies, 77 Va. L. Rev. 881, 916, 934 (1991).

[233] Id. at 916, 934.

sion."[234] Further, this balance must be weighed over time: the court must consider the extent to which each step in the execution of the warrant was needed. Each step in the execution of a warrant involves an implicit decision by the government that the step is "worth it" to recover the evidence described in the warrant in light of the intrusion that particular step will cause on the defendant's interests in privacy and security. The overall assessment of reasonableness requires the court to measure the need for each aspect of the process for recovering the evidence.

The difference between ex ante review of probable cause and particularity, on one hand, and the reasonableness of the execution of the warrant, on the other, is something like the difference between when the government can make an arrest and how much force the government can use in making it. The law governing when the government can make an arrest looks only at the government's interest in making the arrest: the law requires probable cause to believe a crime was committed and that person committed it.[235] However, that is a distinct question from how much force the government can use in making the arrest: the latter requires a fact-sensitive balance of how much force is needed to make the arrest given the suspect's resistance, deference to officer safety concerns, and other factors.[236] As a result, the government can obtain a warrant ex ante authorizing an arrest.[237] But those warrants do not contain any ex ante restrictions on how much force can be used in making the arrest.

<div align="center">CONCLUSION</div>

Ex ante limitations on the execution of computer warrants have arisen from the best of intentions. The magistrate judges who have devised such restrictions have acted out of a commendable effort to protect Fourth Amendment rights in light of a new world of computer search and seizure. The new facts of computer search and seizure change the basic facts of criminal investigations, and those changes trigger the need for new law. As the Ninth Circuit

---

[234] United States v. Place, 462 U.S. 696, 703 (1983).

[235] United States v. Watson, 423 U.S. 411, 415–18 (1976).

[236] See Scott v. Harris, 550 U.S. 372, 383 (2007).

[237] See Fed. R. Crim. P. 41.

recognized in *United States v. Adjani*, "[a]s society grows ever more reliant on computers as a means of storing data and communicating, courts will be called upon to analyze novel legal issues and develop new rules within our well established Fourth Amendment jurisprudence."[238] Magistrate judges are on the front lines of the new world: they are seeing the changes before the rest of the judiciary.

Although such restrictions reflect the best of intentions, magistrate judges do not have the constitutional authority to impose limits on how warrants are executed to ensure that the resulting searches are reasonable. Where magistrate judges do impose restrictions on how warrants are executed, reviewing courts should recognize that these restrictions have no effect: while the executive branch often will follow such restrictions, it need not do so. Ex ante restrictions on the execution of warrants are also unwise. The factual vacuum of ex ante and ex parte decisionmaking leads such restrictions to introduce constitutional errors that inadvertently prohibit reasonable search and seizure practices. Further, ex ante restrictions prevent the development of ex post rules of reasonableness that appellate courts must create to account for the new environment of computer search and seizure.

In short, magistrate judges should stand down. They should cease placing conditions on the execution of computer warrants, and they should instead let reviewing trial and appellate courts review the reasonableness of warrant execution ex post.

---

[238] 452 F.3d 1140, 1152 (9th Cir. 2006).