In the Supreme Court of the State of Vermont
Docket No. 2010-479

In re Appeal of Application for Search Warrant

Original Jurisdiction

Surreply Brief Amici Curiae of the American Civil Liberties Union Foundation of Vermont, the American Civil Liberties Union Foundation, and the Electronic Frontier Foundation

---

Jay Rorty
Criminal Law Reform Project
ACLU Foundation
1101 Pacific Ave., Suite 333
Santa Cruz, CA 95060
(831) 471-9000
jrorty@aclu.org
Admitted pro hac vice

Jason D. Williamson
Criminal Law Reform Project
ACLU Foundation
125 Broad Street
New York, NY 10004
(212) 549-2600
jwilliamson@aclu.org
Admitted pro hac vice

Hanni M. Fakhoury
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
hanni@eff.org
Admitted pro hac vice

Catherine Crump
Speech, Privacy & Technology Project
ACLU Foundation
125 Broad Street
New York, NY 10004
(212) 549-2600
ccrump@aclu.org
Admitted pro hac vice

Dan Barrett
ACLU Foundation of Vermont
137 Elm Street
Montpelier, VT 05602
(802) 223-6304
dbarrett@acluvt.org

Table of Contents

Table of Cited Authorities

Cases

ARGUMENT

Whether in its briefs or at oral argument, the Petitioner has not presented the Court with any legal authority to demonstrate that judicial officers should be deprived of their longstanding discretion to impose limitations on the scope of searches and seizures, simply because the search involves a computer. On the contrary, the Petitioner's insistence that amici seek a drastic shift in Fourth Amendment analysis, and its treatment of the case law cited by amici in their opening brief, do not stand up to scrutiny. Moreover, in suggesting that a judicial officer may only evaluate the validity of a search warrant in the context of a post facto motion to suppress, the Petitioner ignores the significant barriers to post facto remedies—a reality that further highlights the importance of courts' ability to ensure particularity and probable cause at the front end, thereby lessening the chances that constitutional violations will occur in the first instance.

I. In Upholding the Validity of the Ex Ante Conditions in this Case, the Court Can Rely on Traditional Fourth Amendment Analysis

Just as is it did in its original petition, the Petitioner claims in its Reply Brief that amici are asking the Court to create a new framework for evaluating computer searches. *See* Pet'r's Reply Br. 5. In fact, it is the Petitioner that asks this Court to alter established Fourth Amendment principles by requesting the right to search computers without limitation.

More than fifty years ago, the U.S. Supreme Court cautioned that "the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude." *Stanford v. Texas*, 379 U.S. 476, 485 (1965). The particularity requirement eliminates general searches and ensures that when considering "what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Id.* (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)). Of course, "heightened privacy protections for

computer searches must be 'based on a principle that is not technology-specific,'" Pet'r's Reply Br. 3 (quoting *United States v. Giberson*, 527 F.3d 882, 887 (9th Cir. 2008)), but this truism means that "whatever new challenges computer searches pose in terms of particularity, the ultimate Fourth Amendment standard is the same for both computer and hard-copy searches: reasonableness." *United States v. D'Amico*, 734 F. Supp. 2d 321, 366 (S.D.N.Y. 2010).

A search has *always* been found reasonable only if the corresponding warrant is limited in scope and particularly describes the items to be searched, thereby limiting an officers' discretion to prevent general rummaging. Thus, rather than creating a new "special approach" specific to computer searches, the superior court here followed its constitutional mandate to ensure that nothing is left to the discretion of the officer executing the warrant in deciding what to search and seize.[1] The Petitioner points out that "[i]n searching a house for drugs, a murder weapon, or forged checks pursuant to the appropriate warrant, the officers will be able to look everywhere in the house," Pet'r's Reply Br. 5, but this formulation elides the important limitation "that a search warrant authorizing the seizure of materials also authorizes the search of objects *that could contain those materials*." *Giberson*, 527 F.3d at 886 (emphasis added). Because the nature of digital data makes traditional visual size or shape differentiations impossible, some ground rules must be imposed upon the search in order to avoid permitting the police "to search and seize

1 Moreover, the methods chosen by the superior court here are hardly an innovation of the court's decision *in United States v. Comprehensive Drug Testing, Inc. (CDT)*, 621 F.3d 1162 (9th Cir. 2010). In civil litigation, where electronic discovery has become routine, trial courts have crafted similar approaches in order to ensure access to relevant documents without laying bare entire hard drives. *See Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, 267 F.R.D. 443, 449 (D. Conn. 2010) (appointing neutral forensic expert to conduct imaging of hard drives, "recover and organize the mirrored files in a reasonably searchable form," and provide counsel an opportunity to designate irrelevant or privileged material prior to disclosure); *Ameriwood Indus. v. Liberman*, No. 4:06-cv-524-DJS, 2006 WL 3825291, at *5 (E.D. Mo. Dec. 27, 2006) (same, while mandating that "only the Expert and its employees assigned to this project are authorized by this order to inspect, or otherwise handle" imaged data, and requiring that forensic expert "maintain all information in the strictest confidence"), *amended by* 2007 WL 685623 (E.D. Mo. Feb. 23, 2007) (ordering expert to perform party-agreed search protocol, and to "generate a report for the parties identifying the number of 'hits' generated by each search," provided that the parties "continue to meet and confer to refine the Expert's searches to reduce the number of false positives generated by the searches" thereafter).

whatever and whomever they pleased." *Ashcroft v. Al-Kidd*, 131 S. Ct. 2074, 2084 (2011). "[R]esponsible officials, *including judicial officials*, must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) (emphasis added).[2] The judicial officer's responsibility does not change when it comes to searching a home for a shotgun, or a computer for evidence of identity theft. The judicial officer is required to "minimize[] unwarranted intrusions upon privacy" and is empowered to do that by providing officers with limitations to their search authorization. *Id. Cf. In re D.L.*, 164 Vt. 223, 232, 669 A.2d 1172, 1178 (1995) (sustaining against separation-of-powers challenge judicial participation in criminal inquests, in part on the basis that the court's role is to act as a neutral to "assure[] that inquests are conducted in a way that permits the State to investigate a matter without transgressing on witnesses' liberties"). The Petitioner concedes that a judicial official can craft search limits by specifying what property may be searched and for what purpose. *See* Pet'r's Reply Br. 2. But, elevating form over substance, the Petitioner fails to acknowledge that there is no constitutional difference between "how" a search is conducted and "where, for what, and on what basis" a search can occur. *Id.* By providing detailed instructions on how the search can occur, a judicial official renders the search reasonable by ensuring that it is particular and supported by probable cause. Nothing about computers changes that calculus.

Finally, while the Petitioner claims that "the abrogation of the plain view doctrine does not prevent private documents from being viewed, but only prevents them from being used in a criminal prosecution," that point only highlights the need for the limitations imposed by the

2 The Petitioner is correct to state that an "invasive search of a computer" does not automatically transform a search warrant into a general warrant, *see* Pet'r's Reply Br. 4, but a warrant unjustified by probable cause to search everywhere and everything, with no limit on what is to be scrutinized, *is* a general warrant. *Compare* Warrant Appl. ¶¶ 6-8 (purporting to grant permission to search "any and all computers," on the basis of the bare assertion that "if a computer . . . is found on the premises, there is probable cause to believe [the records sought] will be stored in that computer.").

superior court here. *See* Pet'r's Reply Br. 2. By placing these limits on the search of the computer, the superior court ensured that only a limited number of private documents were inspected by law enforcement. The same is true of the state's point that a "search may be intrusive regardless of who conducts it" because forensic examiners will be considered "state actors" for purposes of the Fourth Amendment. *Id.* at 3; *see also Skinner v. Ry. Labor Exec. Ass'n*, 489 U.S. 602, 614 (1989) (private individual is "state actor" under Fourth Amendment if he "acted as an instrument or agent of the Government."). The only way to protect privacy is to limit the scope of the search to cover specific computers, and folders and documents on that computer, where the evidence is likely to be. *See, e.g., United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (invalidating warrant which "authorized the seizure of virtually every document and computer file" because it "contained no limitations on what documents within each category could be seized or suggested how they related to specific criminal activity.").

The superior court did that here by imposing ex ante conditions specifically designed to narrow the scope of the search appropriately and protect the privacy rights of both the suspect and the non-suspect third parties. Its imposition of those measures was a routine fulfillment of courts' constitutional role in the warrant procedure and hardly one of "those exceptional cases where judicial power is usurped or the court clearly abuses its discretion" meriting extraordinary relief. *Chrysler Corp. v. Makovec*, 157 Vt. 84, 88-89, 596 A.2d 1284, 1287 (1991) (internal quotation marks omitted). The petition must be denied.

II. The Federal Court Decisions Cited by Amici Demonstrate that Ex Ante Conditions Have Been Upheld and Support the Notion that Such Cases, Like This One, Must Be Evaluated on a Case-by-Case Basis

The distinctions that the Petitioner attempts to draw in its Reply Brief regarding the federal case law cited by amici fall short.[3] Rather than diminishing amici's position, as the Petitioner argues, *CDT*, *Carey*, *3817 W. West End*, and *Hunter* bolster it by serving both as prior examples of the imposition of ex ante conditions, and as further indication that determining the appropriateness of such conditions requires a fact-specific analysis of each case.

To be clear, amici have never argued that any or all of the *CDT* conditions are *required* in every computer search case. Rather, amici maintain only that judicial officers are *permitted* to, and should, impose appropriate search protocols in circumstances where, as here, law enforcement seeks broad-ranging authority to search computers and other electronic devices.[4] There, as here, the conditions ensure that the warrant in question meets the particularity and probable cause requirements of the Fourth Amendment.

The Petitioner's assertion that *CDT* "has been superseded, is advisory only, has been rejected by numerous courts, and is factually dissimilar to the case at bar," Pet'r's Rep. Br. 7, is puzzling. As it pertains to this case, *CDT* stands only for the proposition that, in light of the "daunting realities of electronic searches," the issuance of warrants in this context requires "greater vigilance on the part of judicial officers" to guard against the risk of unconstitutional searches and seizures. 621 F.3d at 1177. The decision has not been superseded: while the specific conditions articulated by Chief Judge Kozinski in his concurrence are advisory, the majority

3 The cases include *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010), *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953 (N.D. Ill. 2004), and *United States v. Hunter*, 13 F. Supp. 2d 574 (D. Vt. 1998).

4 One can easily imagine circumstances in which one or more of the conditions are unnecessary (because, for instance, the device to be searched is of limited capacity or functionality), or in which one of the conditions tends to obviate another (such as the neutral third party investigator requirement here likely resulting in the plain view condition never being invoked). Neither of these suppositions buttress the petitioner's assertion that all of the conditions are always impermissible.

opinion remains binding Ninth Circuit law and expressly recognizes that "[e]veryone's interests are best served if there are 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." *Id.* *CDT*'s factual dissimilarity is of no importance to this dispute. Amici do not argue that all of the *CDT* conditions must be blindly superimposed onto every digital search warrant. The unique circumstances of each case make it essential for judicial officers to exercise their authority to craft particularized search protocols on a case-by-case basis.

Petitioner attempts to assail amici's reliance on *Carey* by suggesting that the "inadvertence" requirement discussed in that case is no longer good law. The cases cited in amici's opening brief roundly disprove this contention. Br. Amicus Curiae 17-19. For amici's purposes, *Carey* stands for the important proposition that, rather than relying on an inadequate "file cabinet analogy," courts should recognize that computer searches may require ex ante "conditions and limitations" specific to the computer context, and that courts should "require officers to specify in a warrant which type of files are sought." 172 F.3d at 1275. Hence, although the court makes clear that its decision is "predicated only upon the particular facts of this case" (a position entirely consistent with amici's argument), it is equally clear that *Carey* assumes judicial authority to impose conditions under appropriate circumstances.

Petitioner also casts *In re Search of 3817* as *requiring* particularized protocols in every computer search. The case says no such thing, and amici make no such argument. Rather, the court focused its holding on the facts before it, *id.* at 959-960, and noted that, as is true here, "what the government seeks is a license to roam through everything in the computer without limitation and without standards. Such a request fails to satisfy the particularity requirement of the Fourth Amendment." *Id.* at 962. Thus, *In re Search of 3817* represents yet another example

in which ex ante conditions, while particular to that case, have been upheld by a federal court.

Lastly, the Petitioner's truncated analysis of *Hunter* is also incorrect. In holding that the warrant in question was not a general warrant, the court noted that most portions of the warrant were explicitly governed by a "comprehensive plan for the seizure and search of the items listed in the warrant," including instructions regarding the roles to be played by the executing officers, FBI computer analysts, and the prosecutor, respectively. 13 F. Supp. 2d at 584-585. Contrary to the Petitioner's assertion, only one section of the warrant (Section IV) was insufficiently particularized. But because—and only because—"the government operated as though Section IV was limited by the first three sections," the entire warrant was deemed valid. *Id.* at 585. The state's analysis does nothing other than distract from *Hunter*'s (and amici's) essential points: that "seizure of computer equipment is vulnerable to a particularity challenge," *id.* at 583, and that, as such, "the search warrant itself, or materials incorporated by reference, must have specified the purpose for which the computers were seized and delineated the limits of their subsequent search." *Id.* at 584.

III. Ex Ante Prevention of Fourth Amendment Violations is Preferable to the Very Limited Post Facto Remedies

A person whose Fourth Amendment right against unreasonable search has been violated has two avenues of redress: suppression of the evidence obtained by the search, and a civil suit for damages against the agent conducting the search. Because federal law all but forecloses both of these post facto remedies if the unconstitutional search is conducted pursuant to a warrant, ex ante judicial control of digital searches is a vital—and often the only—means of preventing Fourth Amendment violations before they occur.

The exclusion of evidence procured in contravention of the Fourth Amendment has recently been restricted so as to cast substantial doubt on its utility as a means of protection. In *Herring*

v. United States, the Supreme Court declared that "the exclusionary rule is not an individual right and applies only where it result[s] in appreciable deterrence" of police lawbreaking, 129 S. Ct. 695, 700 (2009), and is now triggered only where police lawbreaking is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 702 (citation omitted) (alteration in original) (internal quotation marks omitted) (overruling *Weeks v. United States*, 232 U.S. 383 (1914); *Mapp v. Ohio*, 367 U.S. 643 (1961)).

The impact of *Herring* as a barrier to redress in digital search cases is illustrated in *United States v. Rosa*, 626 F.3d 56 (2d Cir. 2010). There, the Second Circuit agreed with the defendant that a warrant reciting a boilerplate list of electronic devices and media "'which would tend to identify criminal conduct'" *id.* at 58, was without "the requisite specificity to allow for a tailored search of his electronic media" because it failed to connect the described items to the criminal activity alleged. *Id.* at 62. *Compare* Warrant Appl. ¶ 6 (asserting that probable cause to search an electronic device exists so long as "a computer or electronic medium is found on the premises"). Notwithstanding its unreserved conclusion that "the warrant fails for lack of particularity," *Rosa*, 626 F.3d at 64, the court applied *Herring* to bar exclusion of the incriminating evidence because the police officer who applied for the warrant also executed the search, and was therefore "intimately familiar with the contemplated limits of the search." *Id.* at 65. There is no dispute that the Fourth Amendment remains an enforceable individual right that is violated by insufficiently particular digital search warrants. However, *Herring* neuters the traditional post facto method of remedying the violation and underscores the importance of controlling the invasiveness of the search prior to its occurrence.

With respect to the second method of redress, a civil suit, the doctrine of qualified immunity treats a signed warrant as effectively laundering the constitutional violation. Police agents

conducting a search that violates the Fourth Amendment will be entitled to qualified immunity from damages unless "the warrant application is so lacking in indicia of probable cause as to render official belief in its existence unreasonable," *i.e.*, "the same standard of objective reasonableness . . . applied in the context of a [good faith reliance] suppression hearing in *Leon*." *Malley v. Briggs*, 475 U.S. 335, 344-345 (1986) (citing *United States v. Leon*, 468 U.S. 897, 922 (1984)). The police officer enjoys such a broad shield against damages because guaranteeing the conformance of the warrant to the Fourth Amendment "*is the magistrate's responsibility* . . . an officer cannot be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient." *Leon*, 468 U.S. at 921 (emphasis added). The wronged digital property owner, however, will frequently fall victim to the broad gap between what the Fourth Amendment requires in the form of minimum particularity and what *Leon* deems to be patently invalid. *See, e.g., United States v. Tracey*, 597 F.3d 140, 149, 152 (3d Cir. 2010) (invalidating warrant for search of electronic devices on particularity grounds where enumeration of items to be searched not contained within the warrant application, but applying good faith exception because warrant not facially invalid); *United States v. Otero*, 563 F.3d 1127, 1132-1134 (10th Cir. 2009) (same for 'any and all' enumeration of devices to be searched). Given the division of responsibility and immunity in which the neutral magistrate bears the responsibility for ensuring that an issued warrant meets the Fourth Amendment's requirements and the police officer is effectively judgment-proof for executing that warrant, it is entirely acceptable for the magistrate to impose limits upon a search prior to its execution in order to avoid a violation of constitutional rights.

IV. Conclusion

Because the limitations placed upon the search warrant by the superior court enjoy ample support under the Fourth Amendment, and the limitations are both reasonable and practical, the petition for extraordinary relief must be denied.

Respectfully submitted,

Jay Rorty
Criminal Law Reform Project
ACLU Foundation
1101 Pacific Ave., Suite 333
Santa Cruz, CA 95060
(831) 471-9000
jrorty@aclu.org
Admitted pro hac vice

_____/s/_____
Dan Barrett
ACLU Foundation of Vermont
137 Elm Street
Montpelier, VT 05602
(802) 223-6304
dbarrett@acluvt.org

Hanni M. Fakhoury
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
hanni@eff.org
Admitted pro hac vice

Catherine Crump
Speech, Privacy & Technology Project
ACLU Foundation
125 Broad Street
New York, NY 10004
(212) 549-2600
ccrump@aclu.org
Admitted pro hac vice

Jason D. Williamson
Criminal Law Reform Project
ACLU Foundation
125 Broad Street
New York, NY 10004
(212) 549-2600
jwilliamson@aclu.org
Admitted pro hac vice

Counsel for Amici Curiae

July 11, 2011

Certificate of Compliance

I hereby certify that this brief totals ten pages, excluding the table of contents, table of authorities, signature blocks, and this certificate as permitted by the Court's order dated June 22, 2011. I additionally certify that the electronic copy of this brief submitted to the Court via email was scanned for viruses, and that no viruses were detected.

_____/s/_____
Dan Barrett
ACLU Foundation of Vermont
137 Elm Street
Montpelier, VT 05602
(802) 223-6304
dbarrett@acluvt.org

Counsel for Amici Curiae

July 11, 2011