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

In re Appeal of Application for Search Warrant

Original Jurisdiction

Brief Amicus 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
Pro hac vice pending

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

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

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

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

Issues Presented

page

Table of Contents

Table of Cited Authorities

Cases

Other Authorities

Rules

Treatises

Interests of Amicus Curiae[1]

The American Civil Liberties Union Foundation of Vermont ("ACLU-VT") is a statewide, nonprofit, nonpartisan organization with more than 3,000 members and supporters dedicated to the principles of liberty and equality embodied in the constitutions and laws of Vermont and the United States. The American Civil Liberties Union Foundation ("ACLU") is a nationwide nonprofit, nonpartisan organization with over 550,000 members, dedicated to the defense and promotion of the guarantees of individual rights and liberties embodied in the state and federal constitutions.

The Electronic Frontier Foundation ("EFF") is a non-profit, member supported civil liberties organization based in San Francisco, California, working to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as counsel or amicus in key cases addressing computer crime, electronic privacy statutes and the Fourth Amendment as applied to the Internet and other new technologies, including *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010). With more than 14,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at www.eff.org.

1 No party or counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than Amici Curiae, its members, or its counsel made a monetary contribution to its preparation or submission.

Statement of the Case

In December 2010, the Burlington police began investigating an allegation that a resident of that city had committed identity theft in contravention of Vt. Stat. Ann. tit. 13, § 2030, by applying online for a credit card using the personal details of an elderly upstate New York man. A combination of Internet service provider billing details, motor vehicle records, a witness interview, and the credit card application information—which contained an email address appearing to be the lone suspect's real name—quickly narrowed the scope of the investigation to a Pleasant Street residence where the man resided, and the computer with which he allegedly applied for the credit card.

Shortly thereafter, the detective applied to the superior court for a search warrant pursuant to Vt. R. Crim. P. 41. The warrant application set forth an account of the investigation and appended boilerplate allegations regarding the use of computers to commit certain crimes. Without any tailoring to include facts specific to the Pleasant Street investigation, the form language pasted into the warrant application asked to seize "[a]ny computers or electronic media, including hard disks . . . compact disks . . . cell phones or mobile devices . . . and removable storage devices such as thumb drives [or] flash drives" in the house, Warrant App. Attachment A ¶ 2, because, in the template's recitation, "if a computer or electronic medium is found on the premises, there is probable cause to believe that [evidence of the alleged crime] will be stored in that computer or electronic medium." Warrant App. ¶ 6. The form also stated that although "it is possible that the PREMISES will contain computers that are predominantly . . . owned[] by persons who are not suspected of a crime," those computers should be seized and searched "[b]ecause electronic data can easily be moved between different computers." *Id.* ¶ 8. The application proposed that the superior court grant permission for the police to "conduct an off-site search of" the seized devices, "to take as long as necessary," *id.* ¶ 11, using "whatever data

analysis techniques appear necessary," including having the police "peruse every file briefly." *Id.* ¶ 10.

Acting the same day, the superior court granted the application in part, following the example provided by *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d.1162 (9th Cir. 2010). Specifically, the court's Order required:

1) The exclusion of the "plain view doctrine," such that the government may not rely on said doctrine to seize, copy, or otherwise utilize evidence related to criminal matters other than the identity theft offenses;

2) The restriction of the inspection and investigation of the computer to an independent third party or personnel who are not involved in the investigation;

3) The segregation and redaction of relevant evidence from other information;

4) The nondisclosure of information outside the scope of the warrant to State investigators or prosecutors;

5) The use of techniques that focus on the specific criminal activity under investigation, including time periods, key word searches, and searches of limited file types;

6) The prohibition of government tools that are used to specifically identify well-known illegal files that are not at issue in this case;

7) The restriction of copying of digital evidence to materials relevant to the targeted alleged activities;

8) The return of non-responsive data;

9) The destruction of non-relevant electronic data; and

10) Submission of a sworn certificate from the government that it has destroyed or returned all copies of data that it is not entitled to keep.

The State did not appeal the superior court's decision, opting instead to impound the Pleasant Street suspect's computer and file a Vt. R. App. P. 21(b) petition for extraordinary relief in this Court without performing the searches. After a single justice of the Court denied the Defender General's motion to dismiss the petition, the Court requested that the Defender General

and the ACLU brief in opposition to the State's petition and scheduled the matter for argument.[2]

Summary of Argument

I. Personal computers and other electronic devices have become a mainstay of American life. Not only do more Americans own computers than ever before, our computers contain an unprecedented volume of information regarding, among many other things, medical history, financial status, political affiliations, employment status, sexual orientation, consumer habits, and other highly sensitive and expressive material. Government efforts to characterize computers as mere filing cabinets or luggage ignore that computers are an indispensible communications tool that allows people to read and publish information. Moreover, unlike a storage place for tangible things, a computer retains information in a manner that does not reflect the intention of its user and records and stores information without the user's express instruction to do so. As such, computer searches in the context of a criminal investigation are especially susceptible to devolving into general writs of assistance that enable the government to access vast amounts of information that is outside the scope of the search warrant in question.

II. The conditions placed upon the search by the superior court are authorized under the U.S. Constitution. The Fourth Amendment prohibits general warrants that would authorize a broader search than necessary to achieve the object of a warrant. The prohibition against general warrants reflects the Framers' and interpreting courts' deep respect and concern for personal privacy and their recognition of the potential excesses of law enforcement. Accordingly, the Supreme Court has not limited judicial officers' authority to impose ex ante conditions in a search warrant. To the contrary, judicial officers charged with the review and issuance of search

2 To avoid duplication, the ACLU Foundation of Vermont, ACLU Foundation, and the Electronic Frontier Foundation will address the permissibility of the superior court's order under the Fourth Amendment. The Defender General will separately address the permissibility of the court's order under Vermont law.

warrants clearly have discretion to limit and define the execution of such warrants.

III. The conditions imposed by the superior court are similar to those endorsed in *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d.1162 (9th Cir. 2010) (hereinafter *CDT*). *CDT* is the most recent judicial effort in a series of factually similar cases involving authorization for computer searches. Each condition is appropriately tailored to protect privacy and limit the invasion of privacy attendant to a computer search. The condition requiring law enforcement to forsake reliance on the plain view doctrine is consistent with the special care that must be taken in cases involving potentially relevant evidence that is likely to be comingled with highly personal and sensitive information irrelevant to the investigation. The conditions requiring an independent forensic analysis and limiting communication regarding observations outside the scope of the relevant material are equally necessary for the same purpose. Accordingly, the Petitioner has failed to demonstrate entitlement to extraordinary relief, and the petition must be dismissed.

ARGUMENT

I. SEARCHES OF ELECTRONIC DEVICES IMPLICATE HEIGHTENED PRIVACY INTERESTS

With each passing day, people conduct and store more of their lives on computers, smart phones, and other devices.[3] These devices are far more than receptacles for private files: they have become a commonplace part of the daily life of the average person and a gateway to the Internet and its means of communication, constantly used to help people think, learn, communicate, associate with others and keep track of their own lives and those of their families

3 There is no difference between a computer and a smart phone for Fourth Amendment purposes. Smart phones are "handheld wireless device[s] that function[] as a cell phone, BlackBerry, camera, music player, and video player, while simultaneously providing internet access," Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 U.C.L.A. L. Rev. 27, 29 (2008), with processing and storage capabilities exceeding those available in the computers of ten years ago.

and friends. *See generally* Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 Widener L.J. 667 (2006). A consequence of this new reality is that these devices also maintain a nearly indelible record of everything their users think or search for, what they learn or read, what they say to others, and with whom they associate. It should therefore come as no surprise that "for most people, their computers are their most private spaces." *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting). Two conditions, in particular, distinguish electronic devices from tangible things and require judicial officers hearing search warrant applications to consider the heightened privacy interests in data on those devices: the unprecedented volume of personal information stored on such devices and the significant differences between electronic devices and other kinds of "containers" used to store information.

A. Computers and Smart Phones Contain Large Volumes of Personal Information and Expressive Material

The vast quantity of uniquely private information contained on computers magnifies the privacy and dignity concerns implicated by a search. A computer "is akin to a vast warehouse of information," and a typical hard drive sold in 2005 can carry data "roughly equivalent to forty million pages of text—about the amount of information contained in the books on one floor of a typical academic library." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005). Such a vast quantity and variety of information increases the likelihood that highly personal information will also be searched, seized, or copied during a government inspection of the device.

While the meaning of the probable cause requirement remains the same whether or not a search targets expressive materials, *New York v. P.J. Video, Inc.*, 475 U.S. 868, 875 (1986), expressive interests must be taken into account in determining what protections are necessary to make the search reasonable. "A seizure reasonable as to one type of material in one setting may

be unreasonable in a different setting or with respect to another kind of material." *Roaden v. Kentucky*, 413 U.S. 496, 501 (1973). As *Roaden* held, seizures of expressive materials, such as "books and movie films," are "to be distinguished from" seizures of "instruments of a crime" or "contraband" in appraising reasonableness "in light of the values of freedom of expression." *Id.* at 502, 504. *See also Maryland v. Macon*, 472 U.S. 463, 468 (1985) ("First Amendment imposes special constraints on searches for and seizures of presumptively protected material."); *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 326 n.5 (1979) (same). Therefore, the Fourth Amendment's procedural protections must be applied with "scrupulous exactitude" when a search implicates expressive materials. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978). *See also Marcus v. Search Warrants*, 367 U.S. 717, 731 (1961). *See generally United States v. U.S. District Court (Keith)*, 407 U.S. 297 (1972).

B. Computers are Not Closed Containers or File Cabinets

Although the search warrant application at issue in this litigation describes computers as "container[s] for evidence" and "container[s] for contraband," Warrant App. ¶ 7, this is an oversimplification that elides the differences between computers and luggage or filing cabinets. While both are capable of storing personal items, a personal computer is a revolutionary and indispensible communications tool that allows people to read and publish information on the Internet covering a range of topics "as diverse as human thought." *Reno v. ACLU*, 521 U.S. 844, 863 (1997) (The Internet "is the most participatory form of mass speech yet developed, entitled to the highest protection from governmental intrusion.").

In addition, unlike a storage place for tangible things, a computer retains information in a manner that does not reflect the intention of its user. During the course of their operation, computers record and store information without the user's express instruction to do so, such as web browsing history, *see* Warrant App. ¶ 6(c), and hidden repositories of data maintained by the

operating system without the user's knowledge. *See, e.g.,* Nick Bilton, *Tracking File Found In iPhones*, N.Y. Times, Apr. 20, 2011, at B1 (reporting that "Apple face[s] questions . . . about the security of its iPhone and iPad after a report that the devices regularly record their locations in a hidden file"). "A search of a file cabinet, in contrast, would include only items put in the file cabinet by a person." *In re Cunnius*, No. 2:11–mj–00055-JPD-JLR, 2011 WL 991405, at *7 (W.D. Wash. Feb. 11, 2011).

Similarly, it is nearly impossible to effectively remove private information from electronic devices in the same way that one could take it out of a briefcase when one wishes to no longer retain it. "[D]eleted files, or remnants of deleted files, may reside in free space or 'slack space' . . . for long periods of time before they are overwritten," Warrant App. ¶ 6(b), and even such partially overwritten files can be recovered by computer forensic experts. *United States v. Gourde*, 440 F.3d 1065, 1068 (9th Cir. 2006).

Comparisons to closed containers thus vastly oversimplify computers' functions, and ignore the realities of modern existence. Searches of electronic devices implicate heightened concerns of privacy and dignity that distinguish the devices from other types of property subject to compulsory government inspection via search warrant, and it is appropriate for judicial officers to consider those heightened concerns when issuing warrants.

II. THE SEARCH LIMITATIONS IMPOSED BY THE SUPERIOR COURT ARE LAWFUL

The Petitioner's brief asserts that the Fourth Amendment – conceived as a check upon the executive, rather than the judiciary – actually prohibits the superior court from safeguarding individual privacy by narrowing the scope of requested searches. The Fourth Amendment's base requirement of particularity, and ultimate criterion of reasonableness, demonstrate that the superior court was adhering to the law, and that the Petitioner's claim is meritless.

A. The Fourth Amendment Forbids Unconstrained Searches

The Fourth Amendment reflects the Framers' antipathy toward the evils of general warrants, as well as writs of assistance, which authorized British customs officials stationed in the Colonies to conduct broad, generalized searches of private homes at their discretion, in search of any goods that may have been imported in violation of English tax laws. *See Stanford v. Texas*, 379 U.S. 476, 481 (1965). Hence, the Fourth Amendment has long been understood as a "reaction to the evils of the use of the general warrant in England and the writs of assistance in the Colonies," and as an effort to "protect against invasions of 'the sanctity of a man's home and the privacies of life,' from searches under indiscriminate, general authority." *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 301 (1967) (internal citations omitted). *See also McDonald v. United States*, 335 U.S. 451, 455-456 (1948) (explaining that "[p]ower is a heady thing; and history shows that the police acting on their own cannot be trusted. And so the Constitution requires a magistrate to pass on the desires of the police *before* they violate the privacy of the home.") (emphasis added).

Two distinct functions are served by the Fourth Amendment's warrant requirement. "First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Second, the warrant requirement ensures that "those searches that are deemed necessary are as limited as possible," as the evil of unrestrained searches "is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." *Id.* The necessity of a warrant achieves this latter goal by enforcing the so-called particularity requirement of the Fourth Amendment's text, i.e., that "no Warrants shall issue, but . . . particularly describing the place to be searched, and the persons or things to be seized." "By limiting the authorization to search to the specific areas and things for which there is probably cause to search, the requirement ensures that the search will be carefully

tailored to its justifications." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). *See also Marron v. United States*, 275 U.S. 192, 195-196 (1927) (stating that "[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

Accordingly, courts have routinely invalidated warrants whose "description . . . of the place to be searched is so vague that it fails reasonably to alert executing officers to the limits of their search authority," *United States v. Clark*, 638 F.3d 89, 94 (2d Cir. 2011). *See, e.g., Davis v. Gracey*, 111 F.3d 1472, 1479 (10th Cir. 1997) (explaining that warrants are invalid "where the language of the warrants authorized the seizure of virtually every document that one might expect to find in a . . . company's office, including those with no connection to the criminal activity providing the probable cause for the search") (internal quotation omitted); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (same where warrant "contained no limitations on what documents within each category could be seized or suggested how they related to specific criminal activity").

B. Ex Ante Conditions are a Permissible Means of Avoiding Unconstrained Searches

Because it is beyond peradventure that the fulfillment of the particularity requirement is central to establishing the validity of any warrant, issuing courts are required to ensure that authorized searches are appropriately narrow. The particularity of the warrant is an element of its reasonableness, "the ultimate Fourth Amendment standard . . . for both computer and hard-copy searches." *United States v. D'Amico*, 734 F. Supp. 2d 321, 366 (S.D.N.Y. 2010) (applying the Second Circuit's "all-records" business records exception).

The need for tailoring of a potentially over-broad warrant is illustrated by the warrant application at issue here. In it, the police officer sought permission "to search and seize any and

all computers" in the house, on the basis of his bare assertion that "if a computer or electronic medium is found on the premises, there is probable cause to believe [the records sought] will be stored in that computer or electronic medium." Warrant App. ¶ 6. Worse, the police also sought consent to troll "computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime," because "electronic data can easily be moved between different computers." *Id.* ¶ 8. This rationale would lead to an unreasonable result: every computer file in every computer will always be searchable in the off chance it may contain evidence. There would be no limits to these types of searches. The State's rationale would therefore have Vermont judges routinely issue general warrants, the precise thing the Fourth Amendment was enacted to prevent. This analytical failing plagues the particularity discussion in *United States v. Farlow*, relied upon by the Petitioner. There, the district judge opined that the *CDT* conditions "impose extraordinary precautions against police misconduct" without explaining how general warrants would be permissible so long as the police operate in good faith. *United States v. Farlow*, No. CR-09-38-B-W, 2009 WL 4728690, at *6 n.3. The Fourth Amendment's post-search remedies for executive overreaching are not the sole means of policing the police; the ex ante warrant obtainment procedure itself is the principal check against overbreadth.

The imposition of ex ante restrictions on search warrants by magistrates and other judicial officers is not a novel concept, especially as it relates to ensuring probable cause and particularity. There are at least two familiar contexts in which magistrate judges are already permitted to establish conditions on the execution of a given warrant, in order to address the privacy interests of those for whom there is no probable cause to suspect of criminal activity and ensure that the search is limited to those items particularly described in the warrant application. These include the ex ante appointment of a special master for searches of sensitive documents such as attorney's files, *See DeMassa v. Nunez*, 747 F.2d 1283, 1285 (9th Cir. 1984). *See also*

Williams v. Broaddus, 331 F. App'x 560, 562 (10th Cir. 2009) (no violation of the Fourth Amendment where judge examined plaintiff's seized files in camera because appointed special master unavailable). *See generally Deukmejian v. Superior Court*, 162 Cal. Rptr. 857, 103 Cal.App.3d 253, 258 (1980) (describing state-law special master requirement for searches of documents under the control of, a lawyer, doctor, psychotherapist, or clergy who is not suspected of criminal activity); United States Department of Justice, *United States Attorney's Manual* § 9-13.420, 1999 WL 33219862 (U.S.A.M.), at § F (authorizing U.S. Attorneys to utilize special masters). Judicial officers also impose time and duration restrictions on the execution of the search. *See, e.g.*, Vt. R. Crim. P. 41(c)(5)(ii) (requiring warrants to restrict service "between the hours of 6:00 A.M. and 10:00 P.M. unless the judicial officer for reasonable cause shown authorizes execution at other times"); Fed. R. Crim. P. 41(e)(2)(A)(ii) (same, but specifying "daytime").

The State requests that this Court strike the ex ante conditions from the warrant as issued because the superior court lacked authority to impose those conditions. The Petitioner contends that a line of Supreme Court cases limits the authority of judicial officers reviewing search warrant applications to the narrow issues of whether the application supplies probable cause and describes the places to be searched and items to be seized with sufficient particularity. The Supreme Court has, in fact, invested judicial officers with discretion to regulate the execution of warrants in order to protect the privacy of suspects and third parties.

The first of the cases relied upon by the State, *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979), does not speak to the use of ex ante conditions whatsoever. The holding is limited to the unremarkable principle that a judicial officer abandons her neutrality when she actively participates in the execution of the warrant, going so far as to review seized material at the scene of the search and opining, during the course of the search, as to whether the content merits

seizure. *Id.* at 321. *Lo-Ji Sales* does nothing to limit a judicial officer sitting in her chambers from amending a warrant to guide law enforcement execution of the warrant as the superior judge did here.

Dalia v. United States, 441 U.S. 238 (1979) provides no greater guidance or limitation. *Dalia* is, to some extent, a reverse image of this case. Dalia argued that a warrant authorizing the bugging of his offices was invalid because the issuing judicial officer failed to impose ex ante restrictions to the warrant. The Court reasonably found that in order to conduct electronic surveillance (at least employing the technology of the time) it was necessary to enter and plant the devices, so the magistrate impliedly authorized the police conduct. The court concluded that the Fourth Amendment does not require that a Title III electronic surveillance order include the specific authorization to enter covertly the premises described in the order. *Id.* at 256-57.This limited holding in the arena of Title III wiretapping does not serve the State's argument as to the specific type of ex ante restrictions imposed here, especially because the case speaks only to what is required, not what is prohibited.

The Court's decision in *United States v. Grubbs*, 547 U.S. 90 (2006) also offers no support for the Petitioner, as it deals with the form of the warrant rather than its substance. The issue in *Grubbs* was whether the Fourth Amendment's particularity requirement mandates that the triggering conditions for an anticipatory warrant be set forth on the face of the warrant in order for the warrant to be valid. Answering in the negative, the Court explained that, for whatever its substantive requirements, the particularity requirement identifies only two things "that must be particularly described *in the warrant*: the place to be searched and the persons or things to be seized." *Id.* at 98 (emphasis added) (internal quotations and alterations omitted). Thus, warrants cannot be struck as patently deficient for failing to recite things unconnected to descriptions of the place to be searched or the things to be seized, such as leaving out "a

specification of the precise manner in which they are to be executed," or for omitting "the magistrate's basis for finding probable cause, even though probable cause is the quintessential precondition to the valid exercise of executive power," *id.* (Internal quotations omitted). But *Grubbs* does not alter the constitutional imperative that each warrant provide "written assurance that the Magistrate actually found probable cause to search for, and to seize, every item mentioned in the affidavit," *Groh v. Ramirez*, 540 U.S. 551, 560 (2004), and certainly does not restrain a judicial officer from approving a search narrower in scope than that requested by the applicant. *Id.* at 561. *Cf. Albitez v. Beto*, 465 F.2d 954, 956 (5th Cir. 1972) (warrant-issuing magistrate's duty to act as a detached neutral does not mean that she is required "to 'rubber stamp' conclusory allegations, but to require adequate factual details or underlying circumstances. Neither does 'detached' mean that he must remain mute, and simply accept or reject an affidavit.") (internal quotation omitted).

The Petitioner places similarly misguided reliance on *Richards v. Wisconsin*, a case declining to adopt a per se rule excusing police from the knock-and-announce rule when executing search warrants in felony drug investigations. 520 U.S. 385, 393-394 (1997). Instead, *Richards* established that suppression on the basis of a no-knock failure is a post-hoc, case-specific review of the circumstances at the scene of the warrant's execution to determine whether the police decision was reasonable in hindsight because of a particular danger present there. *Id.* at 394. *Richards* concerns itself solely with the manner in which a search warrant is executed by the police at the location of the property or person to be searched. It and other no-knock cases proliferate in recent Fourth Amendment jurisprudence because, as the Court later explained, "[t]he Fourth Amendment says nothing specific about *formalities in exercising a warrant's authorization*, speaking . . . simply in terms of the right to be 'secure . . . against unreasonable searches and seizures.' Although the notion of reasonable execution must therefore be fleshed

out, we have done that case by case, largely avoiding categories and protocols for searches." *United States v. Banks*, 540 U.S. 31, 35-36 (2003) (emphasis added).

The attempt to describe these cases taken together as a coherent statement barring the imposition of ex ante warrant conditions fails. This case (if decided on federal constitutional grounds), or one like it, may ultimately lead the Court to specifically delineate the boundaries of judicial officers' authority to impose ex ante conditions in computer search cases. But it has not done so yet, and certainly not in the cases relied on by the Petitioner. Thus, the Petitioner's allegation that the superior court followed a special approach to the warrant at issue rings hollow. The conditions upon which the warrant was granted were an acceptable means of ensuring that "nothing is left to the discretion of the officer executing the warrant" in deciding what to search and seize, *Stanford*, 379 U.S. at 485, and the State's petition must therefore be dismissed.

III. THE LIMITATIONS PLACED ON THE SEARCH WARRANT HERE ARE REASONABLE AND PRACTICAL

The issue presented by this case is one that is the subject of a parallel academic debate, engendered by the Ninth Circuit's decision in *CDT*. Professor Orin Kerr protested the *CDT* ruling in *Ex ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev 1241 (2010), an article advancing the view that judicial officers should authorize wide ranging warrants and courts should resolve Fourth Amendment questions about those warrants after their execution, in the context of motions to suppress evidence. The Petitioner's brief relies upon Professor Kerr's analysis almost exclusively.

However, Professor Paul Ohm replied to Professor Kerr in a recent article, *Massive Hard Drives, General Warrants and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1 (2011), in which he concluded that judicial officers may impose ex ante conditions on computer searches as needed. If they cannot, they are left with a binary choice: deny all warrants seeking to search

all the contents of a computer, or issue all such warrants without conditions and address, after the fact, the inevitable constitutional violations that will flow from the execution of those warrants. In Ohm's view, ex ante restrictions are the only practical method of regulating the execution of warrants to search digital devices with comingled evidentiary and non-evidentiary data.

Like Professor Ohm, Amici suggest that ex ante conditions are necessary steps towards ensuring sufficient particularity, because "they are designed to cure the *manifest lack of probable cause and particularity* in almost every computer case." Ohm at 4 (emphasis in original). However, this Court need not decide whether the *CDT* conditions were *required* here. Rather, this Court need only decide whether the conditions were reasonable given the information included in the application. Because the conditions were reasonable, the petition for extraordinary relief is baseless and must be denied.

A. *CDT* Simply Applies Preexisting Fourth Amendment Law to Computer Searches

In *CDT*, the Ninth Circuit dealt with government appeals of three orders compelling the return of seized data and the quashal of a grand jury subpoena for the same data. While possessing probable cause and judicial authorization to seize drug testing records of approximately ten Major League Baseball players suspected of using steroids, the government exceeded the bounds of its probable cause and seized and searched all of the laboratory data showing major league players' steroid test results, contravening existing Ninth Circuit case law requiring minimization measures to be employed when executing electronic searches.

Affirming district court orders compelling return of the data and granting quashal of a pending subpoena, the en banc court warned that the "need of law enforcement for broad authorization to examine electronic records" created a "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id.* at 1176. Central throughout *CDT* is the recognition that computer

searches seem inevitably to require government agents to search through intermingled records, which may contain information law enforcement agents are unauthorized to examine under the search warrant in question. The Ninth Circuit looked to its earlier decision in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982) in disapproving "the wholesale seizure for later detailed examination of records not described in a warrant" as "significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the Fourth Amendment was designed to prevent.'" *Id.* at 595 (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980)).

In a concurring opinion, Chief Judge Kozinski and four colleagues set forth guidelines to ensure "the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects." *CDT,* 621 F.3d at 1178 (Kozinski, C.J., concurring).[4] He cautioned that "[d]istrict and magistrate judges must exercise their independent judgment in every case, but heeding this guidance will significantly increase the likelihood that the searches and seizures of electronic storage that they authorize will be deemed reasonable and lawful." *Id.* Chief Judge Kozinski articulated the following conditions:

1. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.

2. Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.

3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.

4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.

5. The government must destroy or, if the recipient may lawfully possess it, return non-

4 Chief Judge Kozinski's concurring opinion was once part of the majority en banc opinion, but was moved to a concurring opinion upon the issuance of the Court's amended opinion.

> responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1180 (citations omitted). These factors simply provide guidance to law enforcement and judges to ensure that a computer search is "reasonable" under the Fourth Amendment by avoiding a general rummaging through private and personal data. The superior court's use of these factors was a reasonable means of avoiding such a result.

B. Courts Have Imposed Limits on Electronic Searches Long Before *CDT*

Before *CDT*, courts recognized that the sheer scope of information stored on a computer meant making a computer search "reasonable" required limitations on the extent of the search. In other words, before *CDT*, courts applied traditional Fourth Amendment concepts to electronic searches.

The Tenth Circuit has long required law enforcement to limit the scope of computer searches. For example, in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), the police obtained a search warrant to search the defendant's computer for documentary evidence of drug dealing. *Id.* at 1270, 1272-73. The government argued—as the State does here—that the plain view doctrine justified the search because "any file might well have contained information relating to drug crimes and the fact that some files might have appeared to have been graphics files would not necessarily preclude them from containing such information." *Id.* at 1272. The government also argued that "this situation is similar to an officer having a warrant to search a file cabinet containing many drawers. Although each drawer is labeled, he had to open a drawer to find out whether the label was misleading and the drawer contained the objects of the search." *Id.* at 1274.

The circuit court rejected this argument finding the file cabinet analogy "inadequate." *Id.* Noting that "electronic storage is likely to contain a greater quantity and variety of information than any previous storage method," it found "analogies to closed containers or file cabinets may

lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'" *Id.* at 1275 (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 104 (1994)). Finding the search unjustified under the plain view doctrine, it found the scope of the search exceeded the warrant and therefore suppressed the evidence. *Carey*, 172 F.3d at 1276.

Since *Carey*, the Tenth Circuit has repeatedly noted that "officers conducting searches (and the magistrates issuing warrants for those searches) cannot simply conduct a sweeping, comprehensive search of a computer's hard drive." *United States v. Wasler*, 275 F.3d 981, 986 (10th Cir. 2001) (citing *Carey*, 172 F.3d at 1275). *See also United States v. Campos*, 221 F.3d 1143, 1148 (10th Cir. 2000) ("our opinion in *Carey* notes several important limitations on the scope of computer searches of which the parties should be aware."); *United States v. Barbuto*, No. 2:00CR197K, 2001 WL 670930, *5 (D. Utah. April 12, 2001) (recognizing "the important limitations on the scope of computer searches," in *Carey* that require "a more particularized inquiry"). This is consistent with the Supreme Court's instruction that when it comes to searches, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Andresen v. Maryland*, 427 U.S. 463, 482 n. 11 (1976) (emphasis added).

Another example of a judge imposing ex ante conditions prior to *CDT* is provided by *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953 (N.D. Ill. 2004). There the government sought a search warrant to seize and search computers suspected of containing evidence of tax fraud. *Id.* at 955. Acknowledging the breadth of information stored on a computer and worried that "a computer found during the search of a home likely would contain a wide variety of documents having nothing to do with the alleged criminal activity intermingled with documents that might fall within the scope of the alleged criminal activity," the magistrate required the

government to provide a protocol outlining how it would ensure its search was limited to focus on alleged criminal activity. *Id.*

Since it had the authority to limit the search in order to make it "reasonable," the court explained that a broad warrant authorizing seizure and search of the entire contents of the computer failed "to set forth 'objective standards by which executing officers can differentiate items subject to seizure from those which are not.'" *Id.* at 960 (quoting *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986)). The court was concerned because the warrant "does not specify what objective standards the government proposes to use 'to specify what types of files were sought in the searching of the two computers so that personal files would not be searched.'" *Id.* (quoting *Barbuto*, 2001 WL 670930, at *5).

Even closer to home, the federal district court in Vermont has also recognized that with respect to computer searches, in order to "withstand an overbreadth challenge, 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." *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998). *See also United States v. Mann*, 592 F.3d 779, 786 (7th Cir. 2010) (counseling "officers and others involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described."); *People v. Carratu*, 755 N.Y.S.2d 800 (N.Y. Sup. Ct. 2003) ("In view of the Fourth Amendment's 'particularity requirement,' a warrant authorizing a search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity.") (citing *Carey*).

C. Each of the Conditions Imposed Is a Reasonable Measure to Protect Privacy

Each of the conditions imposed by Judge Kupersmith is independently necessary to protect the privacy of the suspect in this case and of unknown third parties whose personal information would otherwise be subject to review by any officer involved in the search. Taken together the conditions ensure that law enforcement officers will locate, receive and be able to act upon all of the information requested in the application, but no more. The resulting balance between public safety and private rights is consistent with the letter and spirit of the Fourth Amendment.

At the outset, conditions five and six (prohibiting copying the data, requiring the prompt return of data, and the destruction of irrelevant data) are housekeeping measures that are necessary to maintain the integrity of data privacy. Compliance with these conditions is not burdensome for the State.

Conditions two through five are necessary protections whose absence would lead to both an unsupported intrusion and further litigation. If a primary investigator were involved in the search, there would be no way to isolate her subsequent investigation into the newly discovered offense without a lengthy hearing regarding the existence of an independent source for the resulting evidence. Similarly, comingled data or the freedom of independent parties to share information with primary investigators would subvert the court's effort to protect the privacy interests of the affected parties.

Eliminating any of conditions two through five would result in an ex post inquiry of the kind that the *Carey* and *CDT* courts sought to avoid. An after-the-fact judicial review in the context of a suppression motion comes with two evils attached, both of which should lead this court to uphold the conditions imposed here. The ultimate cost and burden to the State, as it struggles to establish either that the original search was reasonable and within an exception to the

exclusionary rule or that it has an independent source of evidence on which a subsequent prosecution is based, is not worth any benefit to public safety. By contrast, upholding the conditions prevents the initial and most significant constitutional violation from occurring in the first instance. As demonstrated above, the harm to privacy interests is complete when the protected material is viewed, not when a prosecution is initiated.

Although the warrant application claims that "a suspect may try to conceal criminal evidence," requiring "searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime," Warrant App. ¶ 10, the Department of Justice has developed sophisticated tools to narrow and limit searches. These techniques reduce the burden on law enforcement in that they mechanize an otherwise laborious process. The tools may also reduce the level of personal intrusion in that fewer officers look at fewer documents because the sorting takes place electronically.

Assuming that courts will allow law enforcement the latitude to search and seize information related to the target suspect and offense, waiving the plain view exception is the only balancing mechanism that will prevent what should be a targeted search from becoming a general warrant. Any lesser solution, such as seeking a second warrant upon the observation of suspect material unrelated to the original search, simply slows the privacy violation by imposing an intermediate step.

D. The Conditions Present No Bar to Effective Law Enforcement

The State's final claim, that the limitations crafted by the superior court judge are "impractical and unnecessarily impede criminal investigations," is also without merit. *See* Pet'r's Br. 26. The State claims that new technology has made it harder to perform searches, because the amount of information a computer stores means there are more places to be searched. But its position fails to recognize that "while computers present the possibility of

confronting far greater volumes of documents than are typically presented in a paper document search, computers also present the tools to refine searches in ways that cannot be done with hard copy files." *In re Search of 3817 W. West End*, 321 F. Supp. 2d at 959. In fact, "computer technology affords a variety of methods by which the government may tailor a search to target the documents which evidence the alleged criminal activity. These methods include limiting the search by date range; doing key word searches; limiting the search to text files or graphics files; and focusing on certain software programs." *Id.* (citing *Carey*, 172 F.3d at 1276). "[T]he existence of these tools demonstrates the ability of the government to be more targeted in its review of computer information than it can be when reviewing hard copy documents in a file cabinet. *In re Search of 3817 W. West End*, 321 F.Supp.2d at 959.

This is not simply hypothetical posturing. In *United States v. Hunter*, a Vermont district court explained in detail the steps taken by federal law enforcement officers and attorneys to minimize intrusions into private documents on a seized computer. 13 F. Supp. 2d 574, 578, 584-585 (D. Vt. 1998). Among other measures, the U.S. Attorney's Office designed a protocol for executing the search, and assigned personnel with no prior involvement in the investigation to execute the search. *Id.* at 578.

Hunter does not illustrate an isolated, extraordinary effort. Law enforcement and other government officials not only possess the tools to conduct a limited and targeted computer search, but also are encouraged and even required to use these tools. *See In re Search of 3817 W. West End*, 321 F. Supp. 2d at 960 (describing Department of Justice policies). *See also In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993*, 846 F.Supp. 11, 13 (S.D.N.Y. 1994) ("the government has acknowledged that a 'key word' search of the information stored on the devices would reveal which of the documents are likely to be relevant to the grand jury's investigation.") (quotations omitted).

Nor is there any reason to believe that Vermont state agencies do not possess the same tools available to federal law enforcement agencies, because the State itself explains in its petition that "complex computer searches are generally conducted by experts at the Vermont Forensic Laboratory (in consultation with the investigators), due to the complexities of computer searches." Pet'r's Br.15. Officers are trained to use "carefully targeted searches" before attempting to expand them. *Id.* In essence, the State's standard practice is to do what the superior court judge required it do in this particular search warrant: have computer experts conduct narrow and specific searches of information related to identity theft only.

The State's desire to make its job easier by simply taking all computers and searching all things on them cannot be justified when it possesses the tools to narrow searches and avoid wholesale intrusions into individuals' privacy. As such, the superior court was correct in requiring the State to carefully tailor its search.

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
Pro hac vice pending

_____/s/_____
Dan Barrett
Staff Attorney
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
Pro hac vice pending

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

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

Counsel for Amicus Curiae
June 17, 2011

Certificate of Compliance

I hereby certify that this brief totals 7,408 words, excluding the statement of issues, table of contents, table of authorities, signature blocks, and this certificate as permitted by Vt. R. App. 32. I have relied upon the word processor used to produce this brief, OpenOffice 3.3, to calculate the word count.

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

Counsel for Amicus Curiae

June 17, 2011