IN THE SUPREME COURT OF THE STATE OF VERMONT

IN RE APPEAL OF APPLICATION FOR SEARCH WARRANT

Supreme Court Docket No. 2010-479

On Complaint for Extraordinary Relief
from the Superior Court of Vermont, Chittenden Criminal Division

---

PETITIONER'S BRIEF

Attorneys for Petitioner State of Vermont:

Thomas J. Donovan, Jr., Esq.
Chittenden County State's Attorney

Andrew R. Strauss, Esq.
Deputy State's Attorney

Chittenden County State's Attorneys Office
32 Cherry Street, Suite 305
Burlington, Vermont 05401
(802) 863-2865

On the brief:

William H. Sorrell, Esq.
Attorney General

Evan P. Meenan, Esq.
Assistant Attorney General

David E. Tartter, Esq.
Assistant Attorney General

Office of the Attorney General
109 State Street
Montpelier, VT 05609
(802) 828-3171

STATEMENT OF ISSUES

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Rules

Other Authorities

STATEMENT OF THE CASE AND FACTS

In this complaint for extraordinary relief, Petitioner State of Vermont challenges *ex ante* restrictions imposed by the judicial officer on the search of a computer, arguing that the officer exceeded his authority and that this new framework of *ex ante* conditions is unnecessary, unjustifiable, and harmful to the legal process and criminal investigations.

On December 1, 2010, Detective Michael Warren of the Burlington Police Department was assigned to investigate an identity theft case transferred by the New York State Police. Printed Case ("PC") at 7. A New York resident reported that someone had fraudulently attempted to obtain multiple credit cards in his name and file an official address change form with the United States Post Office. PC at 8. The investigation uncovered evidence indicating that these transactions were attempted via the internet from a computer located at 145 Pleasant Avenue, Burlington. PC at 8-10.

On December 22, Detective Warren applied for a search warrant for 145 Pleasant Avenue.[1] PC at 1-14. The application included a request to search for any computers or electronic storage media there and, if any such items were found, to search them for evidence of identity theft. PC at 5-6, 12-13, 14. The application also included an affidavit from Detective Warren detailing the investigation and the incriminating evidence. PC at 7-10. The affidavit further described the detective's knowledge and experience involving the use of computers by criminals, including the following:

[1] This warrant was originally submitted on December 9, 2010. PC at 15-28. The judicial officer granted it subject to conditions specified in an attached boilerplate "Order." PC at 15-18. This "Order," however, contained specifics of a prior warrant that had not been changed to reflect the facts of the current warrant: paragraphs 2, 3, and 4 referred to "evidence relating to the threats being investigated," where it should have referred to evidence of identity theft. PC at 17. After this was brought to his attention, the judicial officer issued an "Amended Order" on December 10 which had the correct language in paragraphs 2 and 4, but not in paragraph 3. PC at 29-30. Law enforcement opted to resubmit the entire warrant on December 22, which the judicial officer granted, fixing the error in paragraph 3 of the "Amended Order" by hand. PC at 3.

> In some cases, it is possible for law enforcement officers and forensic examiners to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

PC at 12. The affidavit also detailed the complexities of forensic examinations and the efforts law enforcement already uses to conduct reasonably limited searches. PC at 10-13. Based on these representations, the warrant sought to conduct a search of the entire computer, off-site, using whatever data analysis techniques necessary. PC at 10-13.

The judicial officer found that the affidavit established probable cause for the search but issued a boilerplate "Amended Order"[2] specifying that the application "is granted subject to the conditions listed herein," PC at 2-4, as follows:

1. As a condition for receiving a search warrant to search the subject computer, the State cannot rely upon the "plain view doctrine" to seize any electronic records other than those authorized by this warrant. That is, any digital evidence relating to criminal matters other than the identity theft offenses, may not be seized, copied, or used in any criminal investigation or prosecution of any person.
2. Inspection and investigation of the subject computer must be done by either an independent third party or specially trained computer personnel who are not involved in the investigation while staying behind a firewall, that is, in the absence of other agents of the State, and subject to a ban on copying or communicating to any person or the State any information found on the subject computer other than digital evidence relating to identity theft offenses.
3. Any digital evidence relating to the offenses here being investigated must be segregated and redacted before it is provided to the State, no matter how intermingled it is.

[2] *See* fn. 1.

4. If the segregation is performed by State computer personnel, it is a condition of this warrant that the computer personnel will not disclose to the State investigators or prosecutors any information other than that which is the target of the warrant, that is, digital evidence of the identity theft offenses.
5. The search protocol employed must be designed to uncover only the information for which the State has probable cause, that is the aforesaid alleged offenses, and only that digital evidence may be provided to the State. Techniques to focus the search should include but are not limited to, specific time periods relevant to the alleged criminal activity, key word searches, and limiting the search to specific file types.
6. The government has at its disposal sophisticated hashing tools that allow identification of well-known illegal files (such as child pornography) that are not at issue in this case. These and similar search tools may not be used without specific authorization by the court.
7. Information relevant to the targeted alleged activities may be copied to other media to provide to State agents. No other digital evidence may be so copied.
8. The government must return non-responsive data, keeping the court informed about when it has done so and what it has kept.
9. Any remaining copies of the electronic data must be destroyed absent specific judicial authorization to do otherwise.
10. Within the time specified in the warrant, the State must provide the issuing officer with a return disclosing 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.

PC at 3-4. The "Amended Order" noted that "[i]n setting these conditions, the Court has been guided by" *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (hereinafter, "*CDT*"). PC at 3.

Detective Warren subsequently executed the warrant and seized, but did not search, a personal computer. PC at 31. On December 29, the State filed the current Complaint for Extraordinary Relief, challenging the *ex ante* conditions.

SUMMARY OF ARGUMENT

There is no doubt that modern computers and other electronic storage media have the capacity to store enormous amounts of intermingled information, and that the law pertaining to searches of this media is still in its infancy. But creating out of whole cloth a new framework—abrogating the plain view doctrine and allowing the judicial officer to restrict *ex ante* how the search may be conducted—is error. First, the authority exercised by the judicial officer under this new framework has no foundation in constitutional or statutory law. Second, this new framework is unnecessary, as existing constitutional law, combined with the normal process of allowing this law to develop through fact-based litigation, is sufficient to protect privacy rights in the context of computer searches. Third, this new framework actually impedes legal development, by allowing judicial officers to define reasonableness without the actual facts and based on limited precedent, and by shifting the focus away from the reasonableness of the search and onto law enforcement's adherence to the *ex ante* conditions. Finally, it impinges on the ability of law enforcement to effectively investigate crimes involving electronic storage media. As such, this Court should reject this new framework and strike the boilerplate preconditions imposed by the judicial officer.

ARGUMENT

I. THE AUTHORITY TO IMPOSE THE *EX ANTE* CONDITIONS DICTATING HOW THE SEARCH MUST BE CONDUCTED HAS NO BASIS IN CONSTITUTIONAL OR STATUTORY LAW.

Under our system of separation of powers, the executive branch is generally given authority over matters of law enforcement. *See United States v. Russell*, 411 U.S. 423, 435 (1973) ("execution of the federal laws under our Constitution is confided primarily to the Executive Branch of the Government"). This power includes "investigating crime and deciding whether to prosecute." *In re D.L.*, 164 Vt. 223, 230, 669 A.2d 1172, 1177 (1995). Under the Vermont and United States Constitutions and Vermont statutory law, the judicial branch is provided limited "checks" over this power in order to "minimize the risk of unreasonable assertions of executive authority." *Arkansas v. Sanders*, 442 U.S. 753, 759 (1979). One such "check" is the warrant requirement of the Fourth Amendment, Article 11, and V.R.Cr.P. 41. *See State v. Savva*, 159 Vt. 75, 85, 616 A.2d 774, 779-80 (1991) ("The preference for judicially issued warrants reflects a 'basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government.'") (quoting *Sanders*, 442 U.S. at 759).

The power exercised by the judicial officer in the present case—imposing *ex ante* conditions prohibiting reliance on the plain view exception and specifying how the search is to be conducted—has no foundation in any of these sources of law. Thus, in requiring these preconditions as a prerequisite for the granting of the warrant, the judicial officer exceeded his authority under this particular check, impinging on the power of the executive branch to investigate and prosecute crimes and interfering with the public's

"interest in effective law enforcement." *State v. Sprague*, 144 Vt. 385, 391, 479 A.2d 128, 131 (1984) (citing *Ohio v. Roberts*, 448 U.S. 56, 64 (1980)); *see also In re Inquest Proceedings*, 165 Vt. 549, 550, 676 A.2d 790, 791 (1996) (recognizing "the public's interest in uncovering the truth during criminal investigations"); *Brady v. Dean*, 173 Vt. 542, 545, 790 A.2d 428, 432 (2001) ("Although the separation of powers doctrine does not contemplate an absolute division of authority among the three branches, it does ensure, at a minimum, that no branch will usurp the core functions or impair the independent institutional integrity of another.") (internal quotations and citations omitted). That the judicial officer may have been well-intentioned in attempting to protect privacy rights in the somewhat murky area of searches of electronic media does not free him from the limits of his authority. *See I.N.S. v. Chadha*, 462 U.S. 919, 951 (1983) ("The hydraulic pressure inherent within each of the separate Branches to exceed the outer limits of its power, even to accomplish desirable objectives, must be resisted.").

A. The Fourth Amendment Does Not Provide Authority To Impose These *Ex Ante* Conditions.

Under the United States Constitution, the warrant requirement "check" is created, and thus limited, by the Fourth Amendment, which provides that "no Warrants shall issue, but upon probable cause … and particularly describing the place to be searched, and the persons or things to be seized." This language empowers a judicial officer in reviewing a search warrant to ensure that the affidavit establishes probable cause and that the warrant specifies the place to be searched and the persons or things to be seized. This language, however, does not authorize the judicial officer to otherwise dictate how law enforcement must conduct the search or do away with established constitutional principles such as the plain view exception.

Although there is no United States Supreme Court case directly addressing the constitutionality of *ex ante* restrictions, in general "existing Fourth Amendment doctrine contemplates a surprisingly narrow role for magistrate judges." Orin S. Kerr, *Ex ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241, 1261 (2010). Professor Kerr bases this assessment on several Supreme Court holdings. *Id.* at 1260-77. For instance, a magistrate's actual participation in the execution of a warrant (there, by accompanying the officers to an adult bookstore, reviewing the obscene material seized there, and informing the searching officers of whether or not the materials met the constitutional requirements for obscenity) violates the Fourth Amendment's requirement of a neutral and detached magistrate. *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 321 (1979). Further, the Fourth Amendment does not require that the triggering condition of an anticipatory warrant be particularly described in the warrant. *United States v. Grubbs*, 547 U.S. 90, 97 (2006). Finally, the Fourth Amendment does not require that a wiretap warrant include a specific authorization to covertly enter the target premises to install the surveillance equipment. *Dalia v. United States*, 441 U.S. 238, 256-57 (1979). As the *Dalia* Court stated, "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.'" *Id.* at 257.

Applying these principles here establishes that the judicial officer exceeded his authority under the Fourth Amendment in imposing the *ex ante* conditions. The ten conditions fall into four general groups: (a) condition 1, which prohibits reliance on the plain view exception; (b) conditions 2 to 4, which prohibit the investigators from being

involved in the actual search of the computer; (c) conditions 5 to 6, which place restrictions on the search methods that may be used; and (d) conditions 7 to 10, which specify how responsive and non-responsive data must be handled and reported to the court. *See* PC at 3-4. These conditions pertain to how the search is to be conducted, not to what is to be searched for or where, nor to the probable cause requirement. The Fourth Amendment thus does not provide authority for the judicial officer to impose such preconditions. *See United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999) ("The warrant process is primarily concerned with identifying what may be searched or seized—not how—and whether there is sufficient cause for the invasion of privacy thus entailed.").

B. Article 11 Does Not Provide Authority To Impose These *Ex Ante* Conditions.

The imposition of *ex ante* conditions on the warrant also finds no support in either the text of, or this Court's analysis of, Chapter 1, Article 11 of the Vermont Constitution.

Article 11 reads as follows:

> That the people have a right to hold themselves, their houses, papers, and possessions, free from search or seizure, and therefore warrants, without oath or affirmation first made, affording sufficient foundation for them, and whereby any officer or messenger may be commanded or required to search suspected places, or to seize any person or persons, his, her or their property, not particularly described, are contrary to that right, and ought not to be granted.

This text is similar to the Fourth Amendment in that it requires that the warrant be based on "sufficient foundation" and that the places to be searched and the persons or items to be seized must be "particularly described." Article 11 is also similar to the Fourth Amendment in that it, too, lacks any language authorizing the judicial officer to specify how the search may be conducted or to do away with accepted constitutional principles.

Moreover, while this Court has recognized that Article 11 may grant protections from governmental intrusions beyond those granted in the Fourth Amendment, *see, e.g.*, *State v. Sprague*, 2003 VT 20, ¶¶ 13-20, 175 Vt. 123, 824 A.2d 539 (Article 11 requires particular justification for an exit order in automobile stops, in contrast to the Fourth Amendment, which allows exit orders as a matter of course), it has at the same time declined to impose further specific requirements unsupported by the text of the Article. For instance, in *State v. Meyer*, 167 Vt. 608, 708 A.2d 1343 (1998), the defendant argued that Article 11 prohibited the search of a home pursuant to a valid search warrant if the homeowner is not present. *Id.* at 609, 708 A.2d at 1344. The Court declined to impose this requirement, stating that while "Article 11 has more specific requirements for warrants [than the Fourth Amendment], [it] does not mention the circumstances involved here." *Id.* at 610, 708 A.2d at 1344. The Court also found that "adoption of defendant's position imposes unreasonable restrictions on necessary law enforcement procedures." *Id.* Like in *Meyer*, the text of Article 11 does not support the actions taken by the judicial officer here, and, as will be further explained below, *see* Section III.D, *supra*, those actions "impose[] unreasonable restrictions on necessary law enforcement procedures."

C. Vermont Statutory Law Does Not Provide Authority To Impose These *Ex Ante* Conditions.

The authority to impose the *ex ante* conditions also does not exist in the Vermont Rules of Criminal Procedure. V.R.Cr.P. 41 specifies only that a warrant must detail evidence establishing probable cause for the search and specify "the property or other object of the search and name or describe the person or place to be searched." V.R.Cr.P. 41(c)(1), (2)(A). Rule 41 mandates that, if the judicial officer is satisfied that there is probable cause to believe that grounds for the warrant application exist, "[the] judicial

officer *shall* issue the warrant." V.R.Cr.P. 41(c)(1) (emphasis added). In other words, if the warrant satisfies the particularity requirement and establishes probable cause for the search, the judicial officer has no choice but to issue the warrant. *See, e.g.*, *United States v. Santtini*, 963 F.2d 585, 595-96 (3d Cir. 1992) (rules providing for issuance of arrest warrants are mandatory, leaving court with no discretion to refuse to issue an arrest warrant once probable cause for issuance has been shown). The rule thus provides no authority for the judicial officer to hold the grant of the warrant hostage unless law enforcement agrees to the *ex ante* conditions.

D. The Court's Supervisory Power Does Not Provide Authority To Impose These *Ex Ante* Conditions.

Finally, the authority exercised by the judicial officer here cannot be found in the court's supervisory power. In general, a court may exercise its inherent, or supervisory, power in order to, among other things, "protect the integrity of the judicial system," *Lamell Lumber Corp. v. Newstress Int'l, Inc.*, 2007 VT 83, ¶ 23, 182 Vt. 282, 938 A.2d 1215, and "deter[] illegality," *United States v. Payner*, 447 U.S. 727, 736 n.8 (1980) (internal quotations omitted). This inherent authority is not unlimited, however. For instance, it cannot be used to impinge on a person's lawful rights. *See, e.g.*, *Elwell v. Vermont Communications Marketing Group, Inc.*, 133 Vt. 627, 630, 349 A.2d 218, 220 (1975) ("The general supervisory power of the trial court over its executions cannot be invoked to preclude any execution to which plaintiff may be lawfully entitled … .").

More importantly, it cannot be used to supplement existing Fourth Amendment protections. *Payner*, 447 U.S. at 733-37. In *Payner*, the district court suppressed evidence obtained in violation of a third party's constitutional rights, relying, in part, on the inherent supervisory power of the federal courts. *Id.* at 730-31. The United States

Supreme Court rejected this use of the court's supervisory power. The Court found that the "desire to deter deliberate intrusions into the privacy of persons who are unlikely to become defendants in a criminal prosecution … must be weighed against the considerable harm that would flow from indiscriminate application of an exclusionary rule." *Id.* at 733-34. This "considerable harm" was the "costly toll" that "the suppression of probative but tainted evidence exacts … upon the ability of courts to ascertain the truth in a criminal case." *Id.* at 734. The Court summed up as follows:

> Were we to accept this use of the supervisory power, we would confer on the judiciary discretionary power to disregard the considered limitations of the law it is charged with enforcing. We hold that the supervisory power does not extend so far.

Id. at 737.

Payner is directly on point. Here, in an attempt to ensure the reasonableness of the search, the judicial officer imposed restrictions on how the search was to be conducted that, if violated, would likely result in exclusion of any evidence obtained in violation of the restrictions. But these conditions—imposed prior to the judicial officer learning the exact details and circumstances of the actual search and without the benefit of legal argument from the parties or an extensive body of guiding precedent—went beyond what the Fourth Amendment, Article 11, and Rule 41 require. (Moreover, as further explained below, *see* Section III.C, *supra*, if the restrictions did not in fact exceed existing constitutional and statutory requirements, they are superfluous.). Thus, under *Payner*, the judicial officer cannot rely on the inherent authority of the court in imposing the *ex ante* conditions. As there is no other basis for such an exercise of power, the judicial officer exceeded his authority.

II. THE EXISTING CONSTITUTIONAL FRAMEWORK CAN BE EFFECTIVELY APPLIED TO SEARCHES OF ELECTRONIC MEDIA TO PROVIDE SUFFICIENT PROTECTION FOR INDIVIDUAL PRIVACY.

The standard procedure for examining the constitutionality of a search conducted pursuant to a warrant, including balancing the privacy interests involved, has two steps: (1) prior to the search, the judicial officer ensures that the warrant application presents evidence sufficient to establish probable cause for the search and that it describes with particularity the things to be seized and the place to be searched, and (2) after the search is executed, its reasonableness, and the judicial officer's determinations pertaining to probable cause and particularity, may be examined through the fact-based litigation stemming from a motion to suppress. *See, e.g., State v. Quigley*, 2005 VT 128, ¶¶ 10-21, 179 Vt. 567, 892 A.2d 211. There is no principled reason why this existing framework cannot be effectively applied in the context of computer searches. *See generally* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 Miss. L.J. 193, 205-20 (2005) (rejecting need for "special approach" to computer searches as such searches "are properly governed by traditional Fourth Amendment rules regulating containers and document searches"); David J.S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 Colum. L. Rev. 841, 861-72 (2005), (arguing that traditional Fourth Amendment rules can successfully be applied to digital searches).

First, the particularity requirement can be utilized to protect the privacy interests of innocent third-parties as well as to prevent "a general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (internal citations omitted) (explaining purpose of particularity requirement). As a condition of granting the warrant, the judicial officer will require law enforcement to precisely specify

what electronic information is sought and which electronic media, and where within that media, the search is to be conducted. Thus, if law enforcement wishes to search an entire computer, it must present sufficient evidence justifying this request. For instance, here Detective Warren stated in the warrant affidavit that he knows, based on his training and experience, that suspects often attempt to conceal incriminating computer files by using deceptive file names. *See* PC at 12. This statement justifies a search of the entire computer in this case—which involves a personal computer used presumably only by the residents of the house, all of whom are suspects—but likely would not justify the search of an entire computer owned and operated by a third-party not involved in the crime.

Second, as with every search, privacy rights implicated in computer searches are further protected by the measure of constitutional reasonableness. *See United States v. D'Amico*, 734 F.Supp.2d 321, 366 (S.D.N.Y. 2010) ("[W]hatever 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.") (internal quotations, citations omitted). Reasonableness is best assessed *ex post*, through a motion to suppress, when the full facts and circumstances of the search are known. *See United States v. Farlow*, No. CR-09-38-B-W, 2009 WL 4728690, *6 (D.Me. Dec. 3, 2009) ("In the Court's view, the far preferable approach is to examine the circumstances of each case, to assess the validity of the computer search protocol, to determine whether the police strayed from the authorized parameters of the search warrant, and to hold the police to constitutional standards in the context of a motion to suppress.").

The case of *State v. Dorn*, 145 Vt. 606, 496 A.2d 451 (1985), presents an analogous situation—intermingled business records—and illustrates how the particularity

requirement and *ex post* review can be effectively applied where similar privacy concerns are implicated. In *Dorn*, as part of an investigation into possible welfare fraud, law enforcement obtained a search warrant for the defendant's barn, seeking records of the pharmacy the defendant had operated. *Id.* at 611, 496 A.2d at 453. The warrant authorized a search for "drug price lists" and for "prescriptions and prescription records for Medicaid recipients." *Id.* at 617, 496 A.2d at 457. In executing the warrant, the police seized "prescription receipt logs," which was the form in which the defendant recorded, among other information, prices charged for drugs dispensed. *Id*. at 619, 496 A.2d at 458. Moreover, the investigators discovered that the target Medicaid prescriptions were intermixed with non-Medicaid prescriptions, and, while sorting through these prescriptions, the investigators discovered evidence of differential pricing, for which the defendant was subsequently charged and convicted. *Id.* at 620, 496 A.2d at 459. During the prosecution, the defendant moved unsuccessfully to suppress the prescription receipt log and non-Medicaid prescriptions seized during the search, arguing the warrant did not authorize seizure of these records. *Id.* at 619, 496 A.2d at 458.

In rejecting the defendant's claim, this Court first held that the term "drug price listings" described the prescription receipt log with sufficient particularity to justify seizure under the warrant. *Id.* at 619-20, 496 A.2d at 458-59. The Court noted that under the Fourth Amendment, it is "generally recognized that the particularity requirement must be applied with a practical margin of flexibility, depending on the type of property to be seized, and that a description of property will be acceptable if it is as specific as the circumstances and nature of the activity under investigation permit." *Id.* at 619, 496 A.2d at 458 (internal quotation and citation omitted).

The Court further held that the non-Medicaid prescriptions were properly seized under the plain view exception. *Id.* at 620-21, 496 A.2d at 459-60. In order to carry out the authorized search, the investigators "had to look at the various documents within each box in which the records were kept," noting that in the course of such searches, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *Id.* at 621, 496 A.2d at 459 (internal quotations and citation omitted). Under these circumstances, "[w]e do not hesitate to recognize a 'plain view' exception to scrutiny of unrequested documents in this particular case, where the officers were legally on the premises and where the search was limited to only those boxes in which the requested documents were stored." *Id.* at 621, 496 A.2d at 460.

As *Dorn* illustrates, the existing framework utilizing the requirement of particularity and *ex post* judicial review is sufficient to protect privacy interests in cases such as the one here that involve the search of numerous, intermingled documents.

It is also worth noting that Vermont law enforcement already conducts searches of electronic media in a way that protects individual privacy rights. As Detective Warren's affidavit describes, 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. *See* PC at 12. Moreover, the process begins with "carefully targeted searches," *id.*, and only expands if the search does not uncover the evidence sought, because of, say, the methods that the target of the search used to disguise his files. *See id.* Again, a new framework for searches of electronic media is unnecessary.

III. *CDT*'S NEW FRAMEWORK OF *EX ANTE* RESTRICTIONS AND THE ABROGATION OF THE PLAIN VIEW EXCEPTION IS UNJUSTIFIED AND IS HARMFUL BOTH LEGALLY AND PRACTICALLY.

Not only is this new framework unnecessary, it cannot be justified, either by the *CDT* case that the judicial officer relied on or by the nature of electronic storage. Further, the new framework harms the legal process and impedes criminal investigations.

A. The *CDT* Case Should Not Be Relied On, As It Is Not Binding Authority And Is Factually Dissimilar To This Case.

CDT arose from the federal government's investigation into the Bay Area Lab Cooperative ("BALCO") and the use of steroids in major league baseball. 579 F.3d at 993. During this investigation, the Major League Baseball Players Association ("MLBPA") consented to voluntary, suspicionless drug testing of all major league baseball players, which was administered by Comprehensive Drug Testing. *Id.* The government later obtained a warrant authorizing the search of Comprehensive Drug Testing's offices for the drug-testing records of ten specific players as to whom the government had probable cause to believe had received steroids from BALCO. *Id.* On its own initiative, the magistrate judge granting the search warrant imposed conditions requiring the government to separate these records from the records of all the other major league baseball players who submitted to drug testing. *Id*. at 994. When it executed the search warrant, however, the government did not comply with this condition. Instead, it searched through the records of hundreds of players for whom it did not have probable cause to believe committed any crime. *Id.* at 993–95. The MLBPA subsequently filed civil suits seeking the return of the seized information that was outside the scope of the warrant. *Id.* at 993-94. These challenges led to two district court orders giving the MLBPA what it had requested, based on the fact that the government had blatantly

disregarded the magistrate's limitations on the warrant and "displayed a callous disregard for the rights of third parties." *Id.*

On appeal, the Ninth Circuit en banc upheld the district court rulings, finding that "[t]his was an obvious case of deliberate overreaching by the government in an effort to seize data as to which it lacked probable cause." *Id.* at 1000. In addition to deciding the matters before the court, the majority went on to specify several conditions that magistrates should abide by whenever the government in the future seeks to obtain a warrant for a computer or other electronic storage medium:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it 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-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1006.

Several members of the en banc panel dissented from this latter portion of the majority's opinion, arguing that the suggested guidelines "are dicta and might be best viewed as a 'best practices' manual, rather than binding law"; "are overbroad and restrict how law enforcement personnel can carry out their work without citing to legal authority

that would support these new rules;" and "go[] against the grain of the common law method of reasoned decisionmaking, by which rules evolve from cases over time." *Id.* at 1012-14 (Callahan, J., joined by Ikuta, J., concurring in part and dissenting in part); *id.* at 1018 (Bea, J., concurring in part and dissenting in part). With regard to the proposed condition abrogating reliance on the plain view doctrine, the dissenters argued that "[s]uch a rule departs from existing Supreme Court precedent … and do[es] so without a single citation to the Supreme Court's extensive precedent on the subject or an explanation why that precedent no longer applies." *Id.* at 1017 (Bea, J., concurring in part and dissenting in part); *see also id.* at 1013 (Callahan, J., joined by Ikuta, J., concurring in part and dissenting in part) (same).

The *CDT* case, coming from the Ninth Circuit, is of course not binding here in Vermont state court. More importantly, though, the *CDT* warrant restrictions are not even binding in the Ninth Circuit. As the *CDT* dissent pointed out, the restrictions were not necessary for the outcome of the case and therefore are mere dicta. *Id.* at 1012-13 (Callahan, J., concurring in part and dissenting in part). Moreover, the original *CDT* case has since been superseded by a subsequent rehearing, where the Ninth Circuit withdrew the broad-based endorsement of *ex ante* conditions for computer search warrants and relegated the advisory warrant restrictions to a concurrence. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1165-80 (9th Cir. 2010).[3] Finally, as noted in one of the *CDT* dissents, *CDT*'s preconditions on search warrants contradict

[3] While the Ninth Circuit arguably preserved one of these conditions—the waiver of the plain view doctrine—it still acknowledged that the plain view exception to the search warrant requirement may apply if the government conducts a computer search limited to specified suspects. *Id.* at 1181 ("A valid 'plain view' seizure of items that are truly 'immediately apparent' would have required the agent to display only the testing results for the ballplayers for whom he had a warrant, and seize only evidence of additional illegality if such evidence is 'immediately apparent' as part of the *segregated* results for those ballplayers.").

prior Ninth Circuit precedent in which the court declined to impose heightened Fourth Amendment protections in computer search cases, ruling that such heightened protections must be "based on a principle that is not technology-specific." *United States v. Giberson*, 527 F.3d 882, 887-88 (9th Cir. 2008) (cited in *CDT*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part)). As the *Giberson* court emphasized, "neither the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth Amendment context." *Id.* at 888. The *CDT* majority in fact cited to *Giberson* without overruling it, *see CDT*, 579 F.3d at 1006, indicating that the majority was less concerned with Fourth Amendment jurisprudence than with the government's blatant violations of the original warrant.

Second, the concerns that the *CDT* court was attempting to address through the imposition of *ex ante* conditions are not present here. Unlike in *CDT*, there has been no allegation of bad action on the part of law enforcement here such that these preconditions are necessary to deter future overreaching. *See also Farlow*, 2009 WL 4728690, *6 n.3 ("The *CDT* protocols impose extraordinary precautions against police misconduct for all applications for a warrant to search a computer, assuming misconduct will be the rule, not the exception. There is no evidence that police disobedience of search warrant limitations is so widespread to compel such onerous pre-issuance procedures, and at the very least the more traditional remedies should be tried first.")

More importantly, the present search implicates no third-party concerns. Like many cases in Vermont, the computer at issue here is a personal computer, which presumably contains information belonging solely to the residents of the home, all of whom are possible suspects. There is no indication that any other persons have a privacy

interest in the computer and thus no indication that information pertaining to innocent people will be examined during the search. Indeed, the only third-party interests implicated here are those of the victim, who can only benefit from a search of the computer. In short, the case at bar presents no reason that such heightened (pre)scrutiny of the computer search is necessary.

B. *CDT*'s New Framework For Computer Searches Has Been Explicitly Rejected By Numerous Courts And Implicitly Rejected By The Vermont Supreme Court.

Notably, no other federal circuit court has found that the nature of electronic storage requires the imposition of the sweeping preconditions laid out in *CDT* and adopted by the judicial officer. *See Farlow*, 2009 WL 4728690, at *6 (noting that "no other circuit has gone as far as the Ninth to require such significant preconditions on the issuance of search warrants for computers"); *United States v. King*, 693 F.Supp.2d 1200, 1230 (D.Haw. 2010) (noting that "[t]he *CDT* opinion itself does not claim to base its 'procedures' on the Fourth Amendment"). Further, court after court has explicitly rejected the notion that there is a qualitative difference between electronic storage and other types of storage requiring new constitutional principles. *See, e.g.*, *Upham*, 168 F.3d at 535 (recognizing that "a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs"); *United States v. Williams*, 592 F.3d 511, 523 (4th Cir. 2010), cert denied, 131 S.Ct. 595 (2010) ("At bottom, we conclude that the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents."); *United States v. Fumo*, 565 F.Supp.2d 638, 649 (E.D.Pa. 2008) (acknowledging that "because of the nature of computer files, the government may legally open and briefly examine each file

when searching a computer pursuant to a valid warrant"); *United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, *36 (S.D.N.Y. Apr. 4, 2007) ("At bottom, then, there is neither a heightened nor a reduced level of protection for information stored on computers … ."). And court after court has rejected several of the individual conditions imposed here. *See, e.g.*, *United States v. Mann*, 592 F.3d 779, 785 (7th Cir. 2010) (rejecting *CDT*'s requirements that the plain view doctrine be abrogated in computer searches and that law enforcement obtain pre-approval for search methodology); *Williams*, 592 F.3d at 521 (holding that plain-view exception to warrant requirement applies to searches of computers); *Vilar*, 2007 WL 1075041, at *36 (noting that "the vast majority of courts to have considered the question" have concluded that a warrant need not specify how the computers will be searched; citing cases); *State v. McCrory*, 2011 – Ohio- 546, ¶ 49, 2011 WL 382757, *9 (Ohio Ct. App. Feb. 8, 2011) ("The overwhelming weight of authority is to the effect that warrants need not contain any sort of search protocol, methodology, or other strategy restricting a computer search to specific programs or terms in order to satisfy the particularity requirement."; citing cases).

With regard to Vermont precedent, this Court has repeatedly held that the plain view doctrine applies to home searches even though the home contains a person's most private information and is afforded the highest expectation of privacy by the Vermont constitution. *See, e.g.*, *State v. Mountford*, 171 Vt. 487, 495, 769 A.2d 639, 647 (2000) ("Assuming a lawful entry, the physical evidence found in the living room was in plain view and could properly be seized.") (abrogated on other grounds by *Brigham City v. Stuart*, 547 U.S. 398 (2006)); *State v. Bain*, 2009 VT 34, ¶¶ 3, 14–17, 185 Vt. 541, 975 A.2d 628 (affirming trial court's conclusion that seized marijuana was admissible

because it was in plain view when law enforcement entered defendant's house). There is no principled reason for diverging from this rationale when it comes to electronic media.

A precedent-setting decision involving unwarranted searches under Article 11 also provides guidance here. In *State v. Morris*, 165 Vt. 111, 680 A.2d 90 (1996), this Court held that Article 11 protects persons from warrantless police searches into the contents of secured opaque trash bags left at curbside for garbage collection and disposal. The Court held that "because persons have an objectively reasonable privacy interest in the contents of such containers, police must obtain a warrant before searching through them." *Id.* at 114, 680 A.2d at 93. In doing so, this Court recognized that a search of a person's trash can reveal "intimate details of people's lives," including details about sexual practices, health, personal hygiene, financial and professional status, political affiliations and inclinations, private thoughts, personal relationships, romantic interests, and religious beliefs. *Id.* at 116-17, 680 A.2d at 94. Yet, at no point in the *Morris* decision, or in any other decision, did the Court suggest that warrants of a person's trash must include restrictions such as the abrogation of the plain view exception or the imposition of a barrier between those searching the garbage bags and those investigating the case—despite the fact that "'almost every human activity ultimately manifests itself in waste products,'" *id.* at 116, 680 A.2d at 94 (citation omitted) and that garbage bags, like computers, are likely to contain a wealth of material beyond those specifically sought in the warrant.

The *ex ante* conditions imposed here in fact benefit a criminal who stores incriminating evidence electronically as opposed to a filing cabinet in their home. The conditions go beyond what the Fourth Amendment and Article 11 require, thus providing

protection for illegal computer files beyond that provided for non-computer files. This makes no sense. As one court has stated, "[t]here is no justification for favoring those who are capable of storing their records on computer over those who keep hard copies of their records, however. Computer records searches are no less constitutional than searches of physical records, where innocuous documents may be scanned to ascertain their relevancy." *United States v. Hunter*, 13 F.Supp.2d 574, 584 (D.Vt. 1998). Indeed, "it is precisely because computer files can be intermingled and encrypted that the computer is a useful criminal tool." *Vilar*, 2007 WL 1075041, at *36.

In short, there is no principled reason to distinguish between a search of a person's computer and a search of the same person's trash, or their home, or their office, in this respect. The imposition of a new framework has been soundly rejected across jurisdictions and should be rejected here.

C. The *Ex ante* Regulation Of The Reasonableness Of Computer Searches Introduces Constitutional Error, Impedes The Development Of The Law In This Area, And Is Ultimately Superfluous.

Not only is *CDT*'s *ex ante* regulation of the reasonableness of computer searches unnecessary and unjustified, it is also "unworkable and unwise." Kerr, 96 Va. L. Rev. 1241, at 1277. First, *ex ante* regulations tend to introduce constitutional error into the process, as the judicial officer is acting from within a factual and legal vacuum. In imposing preconditions on a warrant, the officer is attempting to ensure a standard of reasonableness—which is highly factbound—without the facts and circumstances of the actual search and without the expertise of the forensic examiner. *See id.* at 1281-83; *see generally Coolidge*, 403 U.S. at 509-10 (Black, J., concurring) ("The test of reasonableness cannot be fixed by per se rules; each case must be decided on its own facts."). Moreover, these preconditions are imposed in *ex parte* hearings without the

benefit of legal briefing or hearing. *See* Kerr, 96 Va. L. Rev. 1241, at 1282. Further, any such legal briefing or argument may be of little guidance, given the current lack of a solid body of law on the reasonableness of computer searches. The amended order here illustrates well this last point. The judicial officer specifically relied on *CDT* in justifying his boilerplate preconditions, but a review of *CDT* reveals that the Ninth Circuit provided no legal authority to support the preconditions it specified. *See CDT*, 579 F.3d at 1006.

Second, *ex ante* restrictions tend to impair rather than aid the ability of appellate courts to develop legal standards of reasonableness. *See* Kerr, *supra*, at 1287-90. Challenges to the lawfulness of the warrant's execution will focus not on the reasonableness of the warrant's execution, but rather on compliance with the judicial officer's preconditions. *See id.* at 1288; *see also id.* at 1289 n.223 (citing case examples). Thus, the constitutional reasonableness of the search may not be reached by the court and may not even be briefed by the parties. *Id.* at 1289.

In fact, given that the ultimate measure of the constitutionality of the search is reasonableness, the *ex ante* restrictions imposed here have, for all intents and purposes, no legal effect. The case of *Richards v. Wisconsin*, 520 U.S. 385 (1997), is illustrative. There, police officers sought a warrant to search a hotel room for drugs, specifically requesting permission to execute the warrant without first knocking and announcing their presence. *Id.* at 388. The magistrate signed the warrant but explicitly deleted the no-knock portion. *Id.* When the officers executed the warrant, however, they did not announce their presence before entering, due to the circumstances at the time. *Id.* at 388-89. During the prosecution, the defendant moved to suppress the cocaine and cash found in the hotel room on the ground that the police violated the knock-and-announce rule as

well as the magistrate's order. *Id.* at 389. The United States Supreme Court rejected these arguments, concluding that the officers' no-knock entry into the defendant's motel room did not violate the Fourth Amendment. *Id.* at 395. According to the Court, while the officers acted contrary to the magistrate's express rejection of the no-knock request, "this fact does not alter the reasonableness of the officers' decision, which must be evaluated as of the time they entered the motel room," based on the "actual circumstances" that the officers confronted. *Id.* at 395-96. In other words, the magistrate's refusal to allow a no-knock warrant had no effect, as the constitutionality of the officers' actions was ultimately determined in an *ex post* reasonableness inquiry, based on the actual circumstance present at the time of the search.

As in *Richards*, the preconditions imposed on the warrant here will ultimately have no legal effect. Whether evidence obtained during a search of the computer should be suppressed depends on whether law enforcement complied with Fourth Amendment and Article 11 requirements, not on whether it complied with the preconditions. If the restrictions imposed by the judicial officer mirror Fourth Amendment and Article 11 requirements, the restrictions will have been unnecessary. On the other hand, if the restrictions go beyond what the Fourth Amendment and Article 11 require, the restrictions cannot be enforced, as they improperly impinge on the executive branch's power to investigate crimes and on the public's interest in effective law enforcement.

In sum, the *ex ante* conditions imposed here cannot help, they can only harm. Thus, rather than creating a new unjustified framework and imposing boilerplate preconditions on every search of electronic storage media, this Court should allow the reasonableness of computer searches, and the application of the plain view doctrine to

such searches, "to develop incrementally through the normal course of fact-based case adjudication." *Mann*, 592 F.3d at 785 (quoting *CDT*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part)).

D. The *Ex ante* Conditions Are Impractical And Unnecessarily Impede Criminal Investigations.

Finally, the boilerplate *ex ante* conditions imposed by the judicial officer impede law enforcement's ability to effectively investigate this and other crimes. For instance, the requirement that the search must be conducted by a separate examiner without the presence or input of the investigator may result in relevant evidence being missed. The forensic examiner's purpose and skill is to conduct computer searches, not to review data to make a decision as to what is or is not relevant evidence. How would the computer expert know if financial documents relate to a particular fraud case, or if personal letters relate to a particular extortion case? Without guidance from the investigator, who is the person most familiar with the investigation and in the best position to judge whether material is or is not relevant to the investigation, the examiner may miss or disregard relevant evidence. Moreover, guidance from the investigator could actually limit the extent of the search, by informing the examiner that certain avenues need not be examined. And this separation serves no purpose: the forensic examiner is as likely or unlikely to conduct an illegal general search of the computer as the investigator.

Another problem is that, to the extent that the conditions allow the judicial officer to examine and approve the search protocol prior to the search,[4] this is unrealistic, given

[4] The condition pertaining to what search protocols may be used specifies that "[t]he search protocol employed must be designed to uncover only the information for which the State has probable cause … ." PC at 3. This could be read as merely providing a general principle, one that is consistent with law enforcement current practice. It could also be read to require law enforcement to have its protocols pre-approved by the judicial officer.

that judicial officers do not have the expertise of a forensic computer examiner. *See, e.g.*, *Farlow*, 2009 WL 4728690, at *6 n.3 ("Even the most computer literate of judges would struggle to know what protocol is appropriate in any individual case, and the notion that a busy trial judge is going to be able to invent one out of whole cloth or to understand whether the proposed protocol meets ill-defined technical search standards seems unrealistic."). This further hampers law enforcement's ability to conduct an effective search because the search is constrained by the limits of the judicial officer's knowledge.

Moreover, separation between investigator and examiner, and the limitations on what search protocols may be used, eliminates the necessary dynamic nature of the search, i.e., altering, limiting, or expanding the search based on information uncovered discovered during the search. As Detective Warren's affidavit details, law enforcement initially attempts to use "carefully targeted searches," PC at 12, but may use "more extensive searches" if the initial searches do not yield the evidence described in the warrant, because of, say, the way that the target of the investigation has attempted to conceal his incriminating files. *Id.* Any requirement that the search protocol must be specified ahead of time or that the investigator cannot be part of the search would stifle this process. *See, e.g.*, *United States v. Burgess*, 576 F.3d 1078, 1092-95 (10th Cir. 2009) (recognizing that it is unrealistic to require the state to prospectively restrict the scope of a computer forensic examination, which "must remain dynamic"); *United States v. Adjani*, 452 F.3d 1140, 1149-50 (9th Cir. 2006) ("To require such a pinpointed computer search, restricting the search to a [particular] program or to specific search terms, would likely . . . fail[] to cast a sufficiently wide net to capture the evidence sought."); *United States v. Graziano*, 558 F.Supp.2d 304, 314 (E.D.N.Y. 2008) (stating that nothing

requires law enforcement to specify search protocols in computer search warrants and "[t]he reason … is obvious—in most instances there is no way for law enforcement … to know in advance how a criminal may label or code his computer files"); *Vilar*, 2007 WL 1075041, at *38 ("it seems manifestly obvious that any requirement that a computer search be confined by a key-word search protocol would inevitably immunize criminals.").

There are other ways that the conditions impede the prosecution of crimes. Condition 8 is virtually impossible to comply with, given that the current practice is to image the hard drive and analyze the image and that non-responsive data cannot be removed from this image with certainty. Condition 9 prohibits maintaining evidence for appeals, post-conviction relief and civil liability. Condition 10 places an arbitrary time limit on the search, despite the fact that such a search "can take weeks or months." PC at 12; *see, e.g., State v. Nadeau*, 2010 ME 71, ¶¶ 11, 15, 1 A.3d 45 (discussing state forensic lab's extreme backlog and holding that time delay in conducting examination did not justify application of the exclusionary rule).

In short, these boilerplate conditions, imposed regardless of the particular facts of the case as known to the judicial officer, prior to the actual search, and without the expertise of the forensic examiner, serve to hamstring law enforcement, for no benefit.

CONCLUSION

In sum, the conditions the Ninth Circuit imposed and the judicial officer adopted here are the type of broad-sweeping one-size-fits all conditions that fail to provide any meaningful protection that existing search warrant law does not already provide. They do, however, potentially prohibit law enforcement from obtaining evidence that it is legally entitled to possess and prohibit the trial court from conducting a meaningful *ex post* reasonableness evaluation of the forensic examination actually conducted. And they have no authorization is any source of law. As such, the State respectfully requests that this Court strike the *ex ante* conditions the judicial officer imposed on the search warrant.

Dated at Burlington, Vermont on this __ day of _____, 2011.

_____
Andrew R. Strauss
Deputy State's Attorney
Chittenden County State's Attorneys Office

CERTIFICATE OF COMPLIANCE

The undersigned certifies that Petitioner's Brief in Docket No. 2010-479 complies with the word-count limitation of V.R.A.P. 32(a)(7). The number of pertinent words in Petitioner's Brief is 8,882. Microsoft Word was used.

Dated at Burlington, Vermont on this __ day of _____, 2011.

_____
Andrew R. Strauss
Deputy State's Attorney
Chittenden County State's Attorneys Office