No. _____

In The

Supreme Court of the United States

IN RE APPLICATION FOR SEARCH WARRANT

STATE OF VERMONT,

Petitioner,

On Petition For A Writ Of Certiorari To The Supreme Court Of The State Of Vermont

PETITION FOR A WRIT OF CERTIORARI

THOMAS J. DONOVAN, JR.
Chittenden County State's Attorney
ANDREW R. STRAUSS
Deputy State's Attorney
CHITTENDEN COUNTY STATE'S ATTORNEY'S OFFICE
32 Cherry Street, Suite 305
Burlington, Vermont 05401
(802) 863-2865

WILLIAM H. SORRELL
Attorney General
BRIDGET C. ASAY
Counsel of Record
JOHN TREADWELL
Assistant Attorneys General
OFFICE OF THE ATTORNEY GENERAL
109 State Street
Montpelier, Vermont 05609-1001
(802) 828-5500
basay@atg.state.vt.us

COCKLE LAW BRIEF PRINTING CO. (800) 225-6964
OR CALL COLLECT (402) 342-2831

QUESTIONS PRESENTED

The State of Vermont applied for a search warrant to seize and search computers for evidence of identity theft. The magistrate that issued the warrant placed detailed conditions on its execution, including conditions that barred the investigating officers from conducting the search and controlled the search methods that could be used. The warrant conditions required a segregated search team and prohibited the search team from disclosing – to anyone – anything other than evidence identified in the warrant. The State sought review of these conditions in the Vermont Supreme Court. In a split decision, that court approved most of the conditions, including the requirement for a segregated search team and the limits on search methods.

The questions presented are:

(1) Does the Fourth Amendment provide a magistrate authority to place conditions on a search warrant that control the manner in which the search is conducted such that a violation of the conditions makes the search unconstitutional?

(2) Does a magistrate have authority under the Fourth Amendment to mandate that a search be executed by a segregated search team that is not investigating the alleged offenses, and to bar the search team from disclosing evidence of other crimes even though that evidence is found in plain view during the search?

PARTIES TO THE PROCEEDING

Petitioner State of Vermont was the petitioner in the Vermont Supreme Court. The Vermont Office of the Defender General (Matthew Valerio, Defender General) appeared as amicus curiae in the Vermont Supreme Court. The American Civil Liberties Union Foundation of Vermont, the American Civil Liberties Union Foundation, and the Electronic Frontier Foundation also appeared as amici curiae in the Vermont Supreme Court.

There is no respondent. The search warrant was sought, as is typical, by an ex parte application to a state-court judge, with no opposing party. App. 81-82; *see Franks v. Delaware*, 438 U.S. 154, 169 (1978). After the magistrate granted the warrant with conditions, the State petitioned for extraordinary relief in the Vermont Supreme Court. As that court noted, there was no party adverse to the State's petition for extraordinary relief. *See* App. 8 n.6. The amici participated in briefing and argument and opposed the State's position.

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF CONTENTS – Continued

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES – Continued

Page

TABLE OF AUTHORITIES – Continued

The State of Vermont respectfully petitions for a writ of certiorari to review the judgment and decree of the Vermont Supreme Court in this case.

INTRODUCTION

This case concerns the Vermont Supreme Court's sweeping assertion of judicial control over the execution of lawful searches and the conduct of police investigations. As required by the Fourth Amendment, law enforcement officers must and do describe with particularity the *place* to be searched and the *person* or *thing* to be seized in a search warrant application. If the officers establish probable cause, the warrant is granted. Law enforcement officers then decide how to execute the warrant, subject to later judicial review for reasonableness. This is no longer the case in Vermont. The Vermont Supreme Court has interpreted the Fourth Amendment to allow magistrates to control the execution of a search by placing mandatory conditions on a warrant. The court's assumption of authority over a traditional police function is inconsistent with the language of the Constitution and finds no support in the precedent of this Court.

Equally troubling, the Vermont Supreme Court approved conditions that substantially burden law enforcement and threaten to impede criminal investigations while advancing no protected Fourth Amendment rights. The conditions endorsed here required a segregated search team that could only

disclose to investigators evidence identified in the warrant. The conditions are "expressly designed to frustrate the plain view doctrine," App. 64 (Burgess, J., concurring and dissenting), by preventing state agents from seizing or disclosing evidence of a crime that is in plain view – and thus unprotected – during a lawful search. Contrary to the lower court's reasoning, a magistrate cannot impose conditions on a warrant that serve no Fourth Amendment purpose. This Court should grant review and reverse the decision below.

OPINION BELOW

The opinion of the Vermont Supreme Court (App. 1-75) is not yet reported, but is available at 2012 WL 6217042.

JURISDICTION

The judgment of the Vermont Supreme Court was entered on December 14, 2012. The jurisdiction of this Court is invoked under 28 U.S.C. § 1257(a).

The State seeks review of the judgment of the Vermont Supreme Court that denied the State's petition for extraordinary relief in most respects. App. 62. Under Vermont law, a petition for extraordinary relief is a matter of original jurisdiction in the supreme court. Vt. R. App. P. 21. It is the only available path for the State to seek review of the denial or

conditioning of a search warrant. *See* App. 9. The court heard the State's petition, granted limited relief, and denied the other relief requested by the State. The proceeding is complete and the court's disposition of the State's petition is final. The state supreme court's ruling is thus a "final judgment or decree" for purposes of review under § 1257(a). *Cf. In re Warrant to Seize One 1988 Chevrolet Monte Carlo*, 861 F.2d 307, 308-09 (1st Cir. 1988) (district court's denial of seizure was a final judgment for purposes of 28 U.S.C. § 1291); *In re Carlson*, 580 F.2d 1365, 1372-73 (10th Cir. 1978) (denial of application for warrant to search and seize taxpayer assets appealable under 28 U.S.C. § 1291).

The Vermont Supreme Court grounded its decision in the federal constitution. *See* App. 13 ("[T]his case is fundamentally about the reach of the Fourth Amendment."). The state court's interpretation of the Fourth Amendment is reviewable under 28 U.S.C. § 1257(a).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue,

but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

STATEMENT

Vermont police want to search a computer for evidence of identity theft. Police lawfully seized the computer pursuant to a warrant. The issue in this case is whether the magistrate who issued the warrant overstepped his authority by placing detailed conditions on the manner of the subsequent search of the computer, including conditions that effectively abrogate the plain view doctrine.

Investigation and Warrant Application

The Burlington, Vermont Police Department is investigating a case of identity theft. In late 2010, an elderly New York man reported that someone had tried to obtain credit cards under his name and also tried to change his address with the Post Office. App. 85. The false change-of-address form supplied a street address in Burlington, Vermont. *Id*. Other evidence pointed to that same Burlington address and to a man named Eric Gulfield, who lived there. App. 86-87.

In response to a subpoena, Comcast provided the subscriber information for the internet protocol (IP) address linked to one of the false online credit card applications. App. 87. The subscriber with that IP

address was on the same street and close by the address linked to Gulfield. *Id*. The detective quickly learned that this Comcast subscriber had an unsecured wireless network. Using a handheld wireless detector, the Burlington detective concluded that the Comcast subscriber's unsecured network could likely be accessed from Gulfield's nearby residence. *Id*.

The Comcast subscriber allowed the detective to download the router log from her computer. The router log showed the network had repeatedly been accessed by a computer with the assigned name GulfieldProp-PC. App. 88-89.

The detective applied for a warrant to search Gulfield's residence for evidence of the crime of identity theft. App. 81-98. Among the items to be seized, the warrant listed "[a]ny computers or electronic media," including hard discs, cell phones and media devices, and removable storage devices such as thumb drives and zip drives. App. 79, 97. In his supporting affidavit, the detective acknowledged that persons other than Mr. Gulfield lived at the home, and that some computers might be predominantly used or owned by other persons not suspected of a crime. App. 92. He sought permission to search those computers too, because "electronic data can easily be moved between different computers and stored thereon." *Id*.

The detective's affidavit explained that, in his experience, an off-site search by a computer expert was often necessary for accuracy and completeness. App. 92-95. The detective described why searching

electronic media can take weeks or months and identified some technical reasons that expert assistance is needed. *Id*. He explained that in some cases, "carefully targeted searches . . . can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence." App. 94. In other cases, however, the suspect may have mislabeled, hidden, encoded, or attempted to delete files to evade detection. *Id*. The latter cases "may require . . . more extensive searches." App. 94-95. Because of these concerns, the detective stated, the investigators "intend[ed] to use whatever data analysis techniques appear necessary to locate and retrieve the evidence" described in the warrant application. App. 95.

The detective accordingly sought permission to (1) seize the computer hardware and other electronic media believed to contain the evidence described in the application; (2) conduct an off-site search if the agents executing the search concluded that it would be impractical to conduct the search on-site; and (3) take as long as necessary to conduct the off-site search/analysis for the evidence described in the application. App. 95.

Search Warrant and Conditions

A Vermont Superior Court judge granted the warrant application but added ten detailed conditions

for its execution.[1] The magistrate's order states, without further explanation, that "[i]n setting these conditions, the [c]ourt has been guided by" *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009).[2] App. 76.

The conditions are set forth in full in the Appendix. App. 76-78. Among other things, the magistrate provided that the State could not rely on the plain view doctrine to seize electronic records other than those described in the warrant. App. 76. The magistrate required the computer search to be done by persons *not* involved in the investigation, and those computer specialists were to stay behind a "firewall." *Id*. That is, the persons searching the computer were banned from disclosing anything to the investigators other than evidence described in the warrant. The digital evidence had to be "segregated and redacted" before being shown to investigators, "no matter how intermingled." App. 77.

The magistrate imposed other restrictions on how the computer search could be conducted, including

---

[1] The judge amended the order twice because of typographical errors not relevant here. The final amended order contains handwritten corrections shown by strikeout in the Appendix. App. 77. The petition refers to the state judge as the magistrate, consistent with Fourth Amendment usage.

[2] That decision was withdrawn and superseded several months before the magistrate issued the warrant and conditions. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam).

specifying search techniques and banning the use of certain "sophisticated hashing tools" without court permission. *Id*. The magistrate ordered the State, without limitation, to "return non-responsive data" and destroy any remaining copies "absent specific judicial authorization to do otherwise." App. 78.

The warrant conditions did not address what the searchers should do if they came across evidence of other serious crimes or an imminent threat to someone's safety. The persons conducting the search could not, consistent with the conditions, convey this kind of information to prosecutors or investigators. *See* App. 76-78. And consistent with the conditions, even contraband like child pornography, if discovered, would have to be returned.

Vermont Supreme Court Decision

The State sought review of the warrant conditions by the Vermont Supreme Court. No statute or rule provides a right of appeal for the State in these circumstances. But Rule 21 of the Vermont Rules of Appellate Procedure provides an avenue for extraordinary relief when other forms of review are foreclosed. The Vermont Supreme Court accepted the petition for extraordinary relief. Because the State's request for a search warrant was necessarily ex parte, there was no adverse party in the Vermont Supreme Court, but two amici (the Vermont Defender General and the ACLU) opposed the State's position. *See* App. 1-2.

In a 3-2 decision, the Vermont Supreme Court upheld the authority of the magistrate, consistent with the Fourth Amendment, to impose all of the conditions except the direct abrogation of the plain view doctrine. Although the State and amici briefed federal and state constitutional issues, the court viewed the case as "fundamentally about the reach of the Fourth Amendment," and declined to rest its decision on either the Vermont Constitution or "Vermont non-constitutional law." App. 13-14.

In its decision, the court first rejected the State's argument that a magistrate lacks authority to impose conditions that "dictate *how* law enforcement must conduct its search." App. 20-21. Describing this as a "real and important" question, the court reasoned that "ex ante instructions may be a way to ensure particularity." App. 22-24. The court also opined that *ex ante* instructions may be permissible to protect privacy, reasoning that magistrates ensure "not simply that there is a reason to believe evidence may be uncovered but that there is a reason that will justify an intrusion on a citizen's privacy interest." App. 28; *see also* App. 30 ("There is interplay between probable cause, particularity, and reasonableness that judicial officers reviewing a warrant application must consider in authorizing a form of privacy invasion.").

The court did not hold that these particular conditions, or any *ex ante* conditions, were constitutionally required. App. 16; *see also* App. 23 ("Our question is not whether the judicial officer's attempt to reconcile these objectives was recommendable,

much less required.") Although the court viewed the conditions as discretionary on the part of the magistrate, the court held that the State was obligated to adhere to them. *See* App. 17, 51-52.[3]

Turning to the specific conditions challenged by the State, the court held that the first condition, which expressly barred the State from relying on the plain view doctrine, was "unnecessary for privacy protection and inappropriate." App. 33. The condition was unnecessary, according to the court, because other conditions "requiring the segregation of the search from the investigation and limiting the results of the search that can be shared, obviate application of the plain view doctrine." *Id.* Given the other conditions, the investigating officers "will never be in the position to view incriminating evidence unrelated to identity theft offenses." *Id.* The court further held that the magistrate did not have authority "to abrogate a legal doctrine in this way," and thus "pick and choose what legal doctrines would apply to a particular police search." App. 33-34.

---

[3] The court suggested that the magistrate imposed the specific conditions "limiting the search techniques" because "[i]n [his] view, this application did not provide probable cause for such a broad search." App. 54-55. The magistrate did not say that the application lacked probable cause, *see* App. 76-80, and the court's discussion on this point is inconsistent with its statement that it was not addressing whether the conditions were even "recommendable, much less required." App. 23. The dissenting opinion noted that "[n]either probable cause nor . . . particularity is challenged here." App. 69.

Although recognizing that the magistrate lacked authority to abrogate the plain view doctrine, the court nonetheless upheld conditions 2, 3, and 4, which together require "that the search be performed by third parties or trained computer personnel separate from the investigators and operating behind a firewall." App. 34. Any police investigators conducting the search were barred from disclosing information other than that related to identity theft. *Id.* The point of these conditions, as the court acknowledged, was to ensure that the police officers investigating the alleged crime would view "only those files that relate to the suspected criminal activity." App. 37.

The court recognized that the "practical consequences of the instructions may be comparable to an abrogation of the plain view doctrine." App. 37. But the court viewed the mechanism as "critically different," because the officers investigating the crime would not themselves see any evidence that might be in the scope of the plain view doctrine. *Id.* The warrant conditions barred the persons conducting the search from seizing or disclosing any evidence of a crime other than identity theft, even if the plain view doctrine would otherwise have allowed the seizure. App. 76-77.

The court reasoned that these screening practices, which in its view made the plain view doctrine irrelevant, were justified as a protection of personal privacy. App. 41-51. The State argued that the loss of privacy was the same, because the digital files would be viewed by the persons conducting the search. The

court, however, viewed the person conducting the search as a "disinterested third party" and reasoned that "one's relationship with a detached third party will be different than with an investigating officer." App. 46. According to the court, "using a disinterested third party is a natural way to protect a person's interest in who will view personal information." App. 49. And the court rejected the State's concern that cutting the investigators out of the search would undermine the effectiveness of the search. App. 52-53.

Next, the court approved of the conditions that controlled the search techniques and protocols to be used by the (already screened) persons conducting the digital search. The court took issue with the warrant application, which it described as seeking authorization for a "broad, unconstrained search," and reasoned that "narrowing the search could still accomplish recovery of the incriminating evidence." App. 55-56. In the court's view, then, the magistrate had discretion to impose the conditions, and the persons conducting the search could get further approvals for expanded search protocols by "educat[ing] the judicial officer on the need for these methods and obtain[ing] approval." App. 58. The court declined to "second-guess" the magistrate's "discretionary judgment" on this point. *Id.*

Finally, the court approved several conditions that allowed only responsive data to be copied, required any non-responsive data to be returned, and directed copies to be destroyed. App. 59-62.

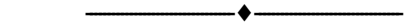
Justice Burgess, joined by Chief Justice Reiber, dissented in part and would have struck conditions 2, 3, and 4. The dissenting justices criticized the majority for acknowledging the plain view doctrine but "turning about-face to uphold conditions that the search be conducted by police agents separated from the case investigators, and who are not to look at, tell about, or must pretend not to see, any plainly visible evidence of other crimes." App. 64. "Whatever limitation the majority invents to prohibit seizure of incriminating evidence in lawful plain view, it is outside of the Fourth Amendment." App. 65.

The dissenting justices explained that upholding the screening conditions did "not . . . vindicate a constitutional right," because the "underlying search warrant is entirely lawful without the . . . gag condition and segregated searchers." App. 67. As the dissenting justices noted, "[n]o one complains that the warrant is insufficiently particular," and the majority "agrees there is no constitutional limitation on observing evidence of other crimes in plain view during a valid search." *Id.* at 67-68. In short, the "majority can point to no infraction of the Fourth Amendment, actual or threatened, to justify its *ex ante* limits on plain view." App. 68.

The dissenting justices took issue with the majority's view that segregating the searches served to protect a privacy interest. Any privacy interest is "already and completely compromised by the warrant and the search," *id.*, and that search is "exactly the same, whether conducted by investigators assigned to

the case, or by the judicially gagged investigators preferred by the majority," App. 69. Likewise, the dissenting judges pointed out that "the majority's assertion that investigators will never view incriminating evidence unrelated to identify theft offenses" is "[p]atently incorrect." App. 69-70. "[T]he other police search team" – the one subject to the gag order – can still view incriminating evidence; they just cannot disclose it. App. 70. "All winking aside, the search is still authorized by the warrant, privacy is still invaded by government search agents, and any other evidence in plain view is still seen." *Id.*

Viewing "the sole purpose of the segregation and gag order" as "discard[ing] the plain view doctrine," the two justices dissented and would have struck conditions 2, 3, and 4. App. 75.



REASONS FOR GRANTING THE PETITION

This Court should grant review to address the Vermont Supreme Court's sweeping assertion of judicial control over the execution of lawful searches and the conduct of police investigations. The Vermont high court's flawed application of the Fourth Amendment raises issues of pressing national importance and has serious consequences for law enforcement. And the lower court's approach in this case departs sharply from the reasoning adopted by several of the federal courts of appeals. The lower court here effectively abrogated the plain view doctrine for digital

searches, an approach that several federal courts have rejected. Likewise, several of the circuits have disapproved of prospective conditions on the execution of digital searches, instead endorsing traditional case-by-case review of reasonableness.

Given the importance of the issue and the fact that the Vermont Supreme Court has departed from the approach endorsed by several federal courts, the Court's guidance is warranted here. This case presents an ideal opportunity to address the propriety of *ex ante* judicial conditions on the execution of a search that is otherwise supported by probable cause.

I. This Court should grant review to address the important and pressing issue of Fourth Amendment law raised by the decision below.

The Vermont Supreme Court has adopted a sweeping and unprecedented view of the authority of a magistrate. Under the court's decision, a magistrate may, by placing conditions on a warrant, dictate the precise manner in which the warrant is executed. The ruling allows the magistrate to prospectively control the conduct of the executing officers; prohibit the investigating officers from conducting the search; and effectively abrogate the plain view doctrine by placing artificial barriers between the executing and investigating officers. The court deemed this approach necessary to limit a perceived intrusion on personal privacy caused by searches of digital files.

In Vermont, as in other states, searches of computers and other electronic devices are a routine and crucial part of law enforcement. Until now, digital searches have been conducted like other searches: if the application is sufficiently particular and supported by probable cause, the magistrate issues a warrant. The reasonableness of the execution of the search – including any application of the plain view doctrine – is tested later, if a defendant challenges the search through a motion to suppress. The decision below dramatically alters this process, giving magistrates new authority to micromanage digital searches. While the court below was the first appellate court to adopt this position, its decision joins a national debate on the permissibility and usefulness of *ex ante* conditions on search warrants. *See*, *e.g.*, *United States v. Comprehensive Drug Testing, Inc.* (*CDT II*), 621 F.3d 1162, 1178-80 (9th Cir. 2010) (en banc) (per curiam) (Kozinski, C.J., concurring); *id.* at 1183-84 (Callahan, J., concurring and dissenting); *United States v. Stabile*, 633 F.3d 219, 240-41 & n.16 (3d Cir. 2011); *United States v. Mann*, 592 F.3d 779, 785-86 (7th Cir. 2010); Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241, 1260-71 (2010).

While *ex ante* conditions are often discussed in the context, as here, of digital searches, this case does not call upon the Court to set standards for reasonable searches of computers and like devices. Those standards are slowly evolving through case-by-case adjudication in the lower courts. The question

presented in this case is whether the case-by-case development of the law should continue, with courts reviewing the reasonableness of digital searches after the fact, based on a concrete record. The Vermont Supreme Court's decision would short-circuit that process, and instead allow individual magistrates to impose mandatory conditions that set the rules for digital searches in advance, with no factual record and little opportunity for judicial review.

The decision below concerns an issue of national importance, has serious immediate consequences for law enforcement, and is based on a flawed understanding of the Fourth Amendment. For all of these reasons, this Court's review is warranted.

A. As evidenced by court decisions and scholarly debate, the authority of magistrates to control the execution of searches through mandatory warrant conditions is a timely and important national issue.

The decision below approved conditions on the execution of a warrant that were drawn from the Ninth Circuit's opinion in *United States v. Comprehensive Drug Testing, Inc.* (*CDT I*), 579 F.3d 989 (9th Cir. 2009) (en banc), *superseded by CDT II*, 621 F.3d 1162. The path of the *CDT* litigation itself confirms that this case poses an issue of national importance.

The *CDT* decisions arose from a federal investigation into steroid use by major league baseball

players. While executing a search warrant for the drug test records of a handful of players, the government seized records for scores of other players. The district court ordered the records returned because the government had blatantly disregarded the magistrate's limitations on the warrant and displayed a "callous disregard" for the rights of third parties. *CDT II*, 621 F.3d at 1167, 1169, 1172.

The government's unsuccessful *CDT* appeal spawned four Ninth Circuit opinions. After two panel decisions, *United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915 (9th Cir. 2006), *superseded by* 513 F.3d 1085 (9th Cir. 2008), the court heard the case en banc. In the first en banc opinion, after ruling against the government, the court set out detailed conditions that magistrates should impose whenever the government in the future sought a warrant for digital evidence.[4] *CDT I*, 579 F.3d at 1000. The conditions drew sharp objections from dissenting judges. *See id.* at 1012-14 (Callahan, J., concurring and

[4] The Ninth Circuit summed up the conditions as (1) "the government [should] waive reliance upon the plain view doctrine in digital evidence cases"; (2) "[s]egregation and redaction [of digital evidence] must be either done by specialized personnel or an independent third party . . . "; (3) "[w]arrants 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) any "search protocol must be designed to uncover only the information for which it has probable cause," and (5) "the government must destroy or, if the recipient may lawfully possess it, return non-responsive data." *CDT I*, 579 F.3d at 1006.

dissenting); *id.* at 1017-20 (Bea, J., concurring and dissenting).

A year later, the en banc court withdrew *CDT I* and in so doing abrogated the proposed search conditions. *CDT II*, 621 F.3d 1162. In *CDT II*, these search conditions are relegated to guidelines in a concurring opinion. *See id*. at 1180 (Kozinski, C.J., concurring); *id*. at 1183 (Callahan, J., concurring and dissenting) ("[T]he suggested guidelines are not Ninth Circuit law.").

CDT sparked national debate about the authority of magistrates to issue *ex ante* conditions and, in particular, conditions limiting the application of the plain view doctrine. Following *CDT I* & *II*, courts around the country have declined to endorse similar conditions. *See* App. 66-67 (Burgess, J., concurring and dissenting) (collecting cases). Two federal circuits have expressly rejected *CDT I*. *See United States v. Stabile*, 633 F.3d 219, 240-41 & n.16 (3d Cir. 2011); *United States v. Mann*, 592 F.3d 779, 785-86 (7th Cir. 2010). This conflict is addressed further in Part II, *infra*. The speed with which this issue has been raised and addressed by other courts confirms its importance.

Scholars have weighed in as well. Professor Orin Kerr addressed the issue in his widely cited 2010 article, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241. Surveying this Court's precedents, Professor Kerr reasons that "existing Fourth Amendment doctrine contemplates a

surprisingly narrow role for magistrate judges." *Id*. at 1261. Professor Kerr concludes that magistrates lack the authority to impose conditions on how warrants are to be executed. If conditions are imposed, they are not mandatory and the executing officers are limited by the constitutional requirement of reasonableness rather than the conditions. Professor Kerr notes that case-by-case review is the most effective way to develop legal standards governing the reasonableness of digital searches. *Id.* at 1293. Other scholars have weighed in with differing viewpoints. *See*, *e.g.*, Paul Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1 (2011) (disagreeing with Kerr about the authority to issue and the need for the *CDT* conditions); Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 Berkeley J. Crim. L. 112 (2011) (recognizing privacy concerns, but concluding that computers should not be subject to greater protections than the home).

Because a magistrate's authority to issue *ex ante* conditions and, in particular, to limit a law enforcement officer's ability to seize items in plain view are matters of substantial national importance, the Court should grant certiorari.

B. Review by this Court is needed to avoid serious consequences for law enforcement and criminal investigations.

Absent review by this Court, law enforcement officers in Vermont have no choice but to adhere to these conditions and similar conditions that magistrates are placing on other warrants. Because the Vermont Supreme Court held that a law enforcement officer who fails to execute a warrant consistent with any conditions imposed on it violates the Constitution, App. 11, 17, 51-52, an officer who does so risks suppression or a lawsuit under 42 U.S.C. § 1983. The court did this even while acknowledging that the conditions themselves are not required by the Fourth Amendment. *See*, *e.g.*, App. 16 ("No party or amicus is directly claiming that *ex ante* instructions are ever required, and we certainly do not hold so here."). The Constitution has never been interpreted to allow magistrates to direct law enforcement activities in this way. *See Dalia v. United States*, 441 U.S. 238, 257 (1979) ("[I]t 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. . . ."); *see also*, *e.g.*, *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.").

This has serious practical consequences for the State. The conditions approved in this case prohibit

the investigating officers from conducting or assisting in the search for relevant evidence. Instead, the State must either hire third parties to conduct the search or use different officers who are screened from the investigators. That requirement alone is expensive, impractical, and unwise. And if the persons conducting the search come across, in plain view, evidence of other serious crime, they may not disclose it to anyone and indeed must return it. The conditions have no exceptions on this point, meaning, for example, that the persons conducting the search would have to return contraband, such as child pornography – even though doing so might itself be a crime.

Moreover, the decision below is not limited to computer searches. It applies to all search warrants, *see* App. 30, and approves conditions on the execution of a warrant *whenever* the magistrate believes the contemplated privacy invasion so requires. App. 24, 26-28. Following the analogy of the digital search conditions at issue here, a magistrate may, for example, dictate which officers may search a building and limit communications among police officers and between police officers and prosecutors. The magistrate may order that officers look first in a desk, and only after that in a filing cabinet. And so on, directing not only where a search may be undertaken and what may be seized, but how the search is conducted. This places the day-to-day supervision of law enforcement investigations with the judiciary, instead of with the police and prosecutors.

This level of judicial involvement and control frustrates the dynamic and iterative process of law enforcement investigations. The conditions require the search team – on pain of invalidating the search – to precisely identify and separate out evidence "relating to identity theft offenses" and disclose *only* that evidence to the investigators. App. 76. And they must do so without the ability to freely discuss the information found with the investigators knowledgeable about the case. This use of "segregated screener-searchers held incommunicado from the primary investigators," App. 65 (Burgess, J., concurring and dissenting), interferes substantially with criminal investigations and creates a serious risk that crucial evidence will be overlooked. Judicially imposed conditions on *how* searches are to be conducted – such as conditions that specify search parameters – erect barriers to the efficacy and speed of investigation with no obvious enhancement of Fourth Amendment rights.

And not least, the Vermont Supreme Court's decision provides uncertain footing for both magistrates and law enforcement in Vermont. It provides no clear standards or limits on the authority of a magistrate to manage a search through *ex ante* conditions. The only guidance provided is the imprecise requirement that the limitations protect privacy interests and relate to the reasonableness of the search. The court observed that it was leaving the nature and extent of a magistrate's authority to impose conditions to another day. App. 16. This Court assigns great weight to readily administrable rules in determining

reasonableness under the Fourth Amendment. *See*, *e.g.*, *Virginia v. Moore*, 553 U.S. 164, 175 (2008). The potential for varied, inconsistent and unreviewable applications of the authority to issue *ex ante* conditions raises serious questions regarding whether the purported additional protections of privacy outweigh the harm to the criminal justice system.

The possibility of future judicial review offers little benefit because – under the court's decision – judicial review of warrant conditions is discretionary and sharply limited. App. 10 (State must show "that the judge's decisions were usurpations of judicial power, *clear* abuses of discretion, or arbitrary abuses of power" (quotation omitted)); *id.* at 23, 58-59 (applying highly deferential standard of review). And appellate review is a prolonged process – this case alone took nearly two years from filing to decision. Case-by-case review of specific conditions is virtually impossible in the context of most criminal investigations. Moreover, for the State to have the conditions reviewed after the fact, police would have to violate the conditions – but the court's opinion directs that violating the conditions "will make the search unconstitutional." App. 11, 17; *see also id.* at 51-52. Absent this Court's review, law enforcement will have little choice but to comply with largely unreviewable conditions that magistrates may choose to impose, or to discontinue investigations if conditions cannot be met. The potential impact on law enforcement activities from such judicial overreach is substantial.

C. The decision below misapplies this Court's precedent and adopts a seriously flawed interpretation of the Fourth Amendment.

The decision below stands as a seriously flawed application of Fourth Amendment jurisprudence. In granting nearly unfettered authority to magistrates to dictate how a search is conducted, the Vermont Supreme Court disregarded both the textual limits of the Fourth Amendment and this Court's precedents. First, the Fourth Amendment calls for a warrant to "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity clause does not give magistrates the further power to control how the search is conducted. The court's contrary holding finds no support in Fourth Amendment precedent. And the court's mandate that these warrant conditions must be followed by police, even if the conditions exceed constitutional requirements, is inconsistent with this Court's guidance. Second, the conditions effectively prohibit the identification and seizure of evidence in plain view. The abrogation of the plain view doctrine is contrary to precedent and undermines effective law enforcement.

1. The court's decision gives magistrates authority that has no source in Fourth Amendment text or precedent.

The court justified the warrant conditions as "mechanisms for ensuring the particularity of a search." App. 24. *But see* App. 69 (Burgess, J., concurring and dissenting) ("[T]he silenced-and-segregated-search-team condition . . . utterly fails to increase particularity. . . ."). That is wrong. The Fourth Amendment demands particularity in two ways – as to the place to be searched and as to the person or thing to be seized. U.S. Const. amend. IV; *United States v. Grubbs*, 547 U.S. 90, 97-98 (2006). This Court has repeatedly "rejected efforts to expand the scope of the particularity requirement to embrace unenumerated matters." *Id.* at 97. In *Grubbs*, the Court reasoned that the Fourth Amendment "does not set forth some general 'particularity requirement'" and held that the "particularity requirement does not include the conditions precedent to execution of the warrant." *Id.* at 97-98. In *Dalia v. United States*, 441 U.S. 238 (1979), this Court observed that neither the Constitution nor precedent required warrants to "include a specification of the precise manner in which they are to be executed." *Id*. at 257.

The court below disregarded this controlling precedent. The particularity requirement does not call for a description of how the person or thing will be found. For that reason, it cannot be the source of authority for warrant conditions – like the ones

approved here – that control how a search is conducted and that *must* be followed by police. Put another way, the Fourth Amendment cannot constitutionalize conditions for executing a warrant when the conditions are not constitutionally required. As noted below, the approved conditions did just this – the segregated-search-team requirement prevents the State from seizing and using evidence that is in plain view and thus unprotected by the Fourth Amendment.

The Vermont Supreme Court relied on three inapposite analogies. First, the court analogized these conditions to a judicial limitation on the location of a search. App. 24. But the requirement that the "place to be searched" be described with particularity is part of the text of the Fourth Amendment. U.S. Const. amend. IV. The Constitution's grant of authority to a magistrate to limit the *location* to be searched does not equate to a grant of authority to specify methods to be used in searching at that location. Second, the court noted search restrictions imposed by federal and state statutes and time limits imposed by rule. App. 25-26, 28-29. The legislature is free to go beyond the Fourth Amendment and impose non-constitutional limitations on law enforcement officers. *See*, *e.g.*, *United States v. Rizzi*, 434 F.3d 669, 675 (4th Cir. 2006).[5] That is a far cry from the judiciary imposing

[5] The time limits for executing a warrant are governed by rule. *See* Fed. R. Crim. P. 41(e)(2)(A)(ii); Vt. R. Crim. P. 41(c)(5)(A)(ii). These rules are "within the scope of the government's police power and are not prohibited or compelled by the Fourth Amendment." *Rizzi*, 434 F.3d at 675; *accord id.* (Supreme Court

(Continued on following page)

additional restrictions not required by the Fourth Amendment but whose violation is deemed to be unconstitutional.

Third, the court reasoned that judicial authorization for a no-knock warrant is analogous to warrant conditions aimed at protecting privacy interests. App. 28-29. The knock-and-announce rule, however, has constitutional force because it is a common law principle that is "an element of the reasonableness inquiry under the Fourth Amendment." *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995). And even so, this Court has held that a magistrate's advance refusal to authorize a no-knock warrant is not binding; rather, the reasonableness of the no-knock entry is evaluated based on the circumstances at the time of execution. *See Richards v. Wisconsin*, 520 U.S. 385, 395-96 & n.7 (1997). None of these examples supports a generalized authority for magistrates to issue conditions that constrain the manner of execution of a warrant and are enforceable under the Constitution if violated.

The warrant conditions accepted below not only lack a constitutional basis, but they blur the constitutional line between the independent magistrate and law enforcement. In *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 327 (1979), this Court disapproved of a magistrate that "allowed himself to become a member, if not the leader, of the search party which was

---

"has never held that the Fourth Amendment prohibits nighttime searches").

essentially a police operation." Dictating the terms of a computer search is the digital equivalent of a magistrate joining a search party. Indeed, here the conditions expressly contemplate further judicial approval for the use of particular search techniques. App. 77 (requiring court authorization before using certain search techniques). The neutral magistrate has a crucial constitutional role as an independent guarantor that constitutional requirements (probable cause and particularity) are met. But the magistrate is not a supervisor of law enforcement functions or a forensic expert.

The Vermont Supreme Court's decision is especially troubling on this point because the court granted power to magistrates to impose conditions that do not serve a Fourth Amendment purpose. Indeed, the court emphasized that it was *not* holding that the magistrate's conditions were constitutionally required. *See* App. 16, 23; *see also* App. 69 (Burgess, J., concurring and dissenting) ("[R]equiring a search by different, segregated and muted investigators serves no Fourth Amendment privacy interest whatsoever."). The imposition of conditions that are mandatory for law enforcement and yet *not* required by the Fourth Amendment cannot be reconciled with *Richards*. There, the defendant argued that the no-knock entry was unreasonable because the magistrate refused to authorize it. This Court disagreed, holding that the magistrate's decision did not "remove the officer's authority to exercise independent judgment" when they executed the search. *Richards*, 520

U.S. at 395-96 & n.7. Whether the search was reasonable did not turn on the magistrate's order, but on the "reasonableness of the officers' decision . . . evaluated as of the time they entered." *Id.* at 395.

2. The segregated-search-team conditions limit law enforcement's access to information that is unprotected under the Fourth Amendment and thus serve no constitutional purpose.

The Vermont Supreme Court properly concluded that it could not require the State to waive the plain view doctrine as a condition of a warrant. App. 30-34. Yet the court simultaneously approved conditions that, as the dissent explained, were "expressly designed to frustrate the plain view doctrine." App. 64 (Burgess, J., concurring and dissenting). As the dissenting opinion correctly recognized, the "gagged search team" requirement does not prevent investigators from seeing evidence in plain view. App. 68-70. The persons who conduct the computer search are state agents carrying out an investigation, whether nominally police officers or not. The conditions mandating segregation of data and strictly limiting disclosure mean that those investigators may not seize or disclose evidence of a crime that is in plain view during a lawful search. In effect, as the dissenting justices recognized, the court imposed a prohibition on plain view. *Id.* It had no constitutional authority to do so.

The observation of an item left in plain view is not a search within the meaning of the Fourth Amendment. *Horton v. California*, 496 U.S. 128, 133 & n.5 (1990); *see also Illinois v. Caballes*, 543 U.S. 405, 408 (2005) ("Official conduct that does not compromise any legitimate interest in privacy is not a search subject to the Fourth Amendment." (quotation omitted)). Where an officer has a prior justification for an intrusion, observes an item, and it is immediately apparent that the item is of evidentiary value, the item may be seized pursuant to the plain view doctrine. *Horton*, 496 U.S. at 135-36.

Although evidence of a crime that is observed in plain view is unprotected by the Fourth Amendment, the court below approved of warrant conditions that prevent law enforcement from seizing those items or disclosing their existence. Those conditions by definition serve no Fourth Amendment purpose. The flaws inherent in the court's conditions can be seen by applying the court's conditions to Justice White's classic hypothetical from *Coolidge v. New Hampshire*, where law enforcement officers obtain and execute a warrant to search a house for a rifle as part of a murder investigation. 403 U.S. 443, 516 (1971) (White, J., concurring and dissenting); *see also Horton v. California*, 496 U.S. at 139. As required, a segregated search team conducts the search. While staying well within the scope of the search for the rifle, the searchers observe two photographs of the murder victim in plain sight in the bedroom. The searchers cannot seize these photographs, cannot disclose their

existence to the investigators, and cannot even apply for a second warrant to seize the evidence. As this example illustrates, the warrant conditions that effectively abrogate the plain view doctrine afford no meaningful constitutional benefit while seriously burdening legitimate law enforcement activity. The privacy intrusion occurs when the search is conducted; the conditions do not limit the intrusion but merely prevent law enforcement from making use of evidence to which they have lawful access. This is a marked departure from existing precedent.

II. The judgment below places Vermont at odds with the governing law of several courts of appeals.

The approach taken by the Vermont Supreme Court departs sharply from the reasoning and holdings of several courts of appeals. As explained above, the court held that a magistrate approving a search warrant may, consistent with the Fourth Amendment, impose conditions that micromanage the execution of a computer search and effectively abrogate the plain view doctrine for digital evidence. Vermont's high court relied upon the reasoning of *CDT I*, which endorsed a similar set of standard search guidelines. *See* App. 17-20; *CDT I*, 579 F.3d at 1006. In doing so, the court adopted a protocol for digital searches that is irreconcilable with the decisions of several courts of appeals. As the Sixth Circuit recently noted, "the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed

the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis." *United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011) (footnote omitted).

Contrary to the decision below, the Seventh Circuit has expressly disavowed *CDT I*. In *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010), the Seventh Circuit rejected the reasoning of *CDT I* and refused to do away with the plain view doctrine for computer searches. *See id.* at 785 (rejecting suggestion "that we take our cue from the more comprehensive rules recently outlined by the Ninth Circuit"). In *Mann*, which predated *CDT II*, the Seventh Circuit aligned itself with Judge Callahan's dissent in *CDT I* and endorsed incremental development of the plain view doctrine "'through the normal course of fact-based case adjudication.'" *Id.* (quoting *CDT I*, 579 F.3d at 1013) (Callahan, J., concurring and dissenting)).

The Third Circuit has also refused to follow *CDT I* or Judge Kozinski's concurring opinion in *CDT II*. In *United States v. Stabile*, 633 F.3d 219 (3d Cir. 2011), the Third Circuit held that the plain view doctrine applies to computer searches, although "the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner." *Id.* at 240-41. Like the Seventh Circuit, the *Stabile* court cited approvingly to Judge Callahan's dissent in *CDT II*, reasoning that, given evolving technology, the Fourth Amendment reasonableness inquiry must be fact-based. *Id.* at 241 n.16.

And both the Sixth and Tenth Circuits have refused to sanction specific computer search protocols for warrants. The Tenth Circuit deemed it "folly for a search warrant to attempt to structure the mechanics of the search" and concluded that "a warrant imposing such limits would unduly restrict legitimate search objectives." *United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009). As the *Burgess* court explained, "[i]t is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, file-name or extension or to attempt to structure search methods – that process must remain dynamic." *Id.* at 1093. The Sixth Circuit in *Richards* followed the reasoning of *Burgess*, agreeing that it is "'folly'" for a warrant to structure the mechanics of a digital search. 659 F.3d at 538 (quoting *Burgess*, 576 F.3d at 1094).

Consistent with these unequivocal rulings, magistrates in the Third, Sixth, Seventh, and Tenth Circuits would not adopt warrant conditions like those imposed in this case.[6] True, each of these decisions

[6] The First Circuit's approach to computer searches is also inconsistent with the reasoning adopted by the Vermont Supreme Court. In *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999), the First Circuit rejected a particularity challenge to a warrant for a computer search. The court reasoned that the search of the defendant's computer and all disks was "about the narrowest definable search and seizure reasonably likely to obtain the [unlawful] images." *Id.* "A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application" and the computer search "is not inherently more intrusive than the physical search of an entire house for a weapon or drugs." *Id.*

(Continued on following page)

reviewed an after-the-fact challenge to a warrant that did not impose conditions on its execution. But while the posture of the cases is not identical, these circuit decisions establish governing law on digital search warrants.[7] The search warrant conditions endorsed by the court below would not be sanctioned in these circuits.

Post-*CDT*, district court decisions in the First Circuit have adhered to *Upham*. *See United States v. Farlow*, No. CR-09-38-B-W, 2009 WL 4728690, at *6 & n.3 (D. Me. Dec. 3, 2009) (criticizing *CDT I* and noting that it "creates more problems than it solves"); *United States v. Burdulis*, No. 10-40003-FDS, 2011 WL 1898941, at **5-7 (D. Mass. May 19, 2011) (following *Upham* and *Farlow*).

[7] Only a decision in the posture of this case – approving the imposition of conditions over the government's objection – could be reviewed in this Court. Because the search warrant application is necessarily ex parte, if a magistrate does not issue conditions, or the government persuades an appellate court to strike them, there is no adverse party to seek review. For this reason as well, this case is an excellent vehicle to consider whether the Fourth Amendment gives magistrates this broad authority.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

THOMAS J. DONOVAN, JR.
Chittenden County
State's Attorney
ANDREW R. STRAUSS
Deputy State's Attorney
CHITTENDEN COUNTY
STATE'S ATTORNEY'S
OFFICE
32 Cherry Street,
Suite 305
Burlington, Vermont 05401
(802) 863-2865

WILLIAM H. SORRELL
Attorney General
BRIDGET C. ASAY
Counsel of Record
JOHN TREADWELL
Assistant Attorneys General
OFFICE OF THE
ATTORNEY GENERAL
109 State Street
Montpelier, Vermont 05609-1001
(802) 828-5500
basay@atg.state.vt.us

March 12, 2013

In re Application for Search Warrant (2010-479)

2012 VT 102

[Filed 14-Dec-2012]

2012 VT 102

No. 2010-479

In re Appeal of Application for Search Warrant	Original Jurisdiction June Term, 2011

Michael S. Kupersmith, J.

Thomas J. Donovan, Jr., Chittenden County State's Attorney, Andrew R. Strauss, Deputy State's Attorney, Burlington, and William H. Sorrell, Attorney General, Evan P. Meenan and David E. Tartter, Assistant Attorneys General (On the Brief), Montpelier, for Petitioner.

Matthew Valerio, Defender General, Rebecca Turner, Appellate Defender and Marshall Pahl, Montpelier, for Amicus Curiae Office of the Defender General.

Dan Barrett, Montpelier, for Amicus Curiae American Civil Liberties Union Foundation of Vermont, Catherine Crump and Jason D. Williamson, New York, New York, and Jay Rorty, Santa Cruz, California, for Amicus Curiae American Civil Liberties Union Foundation, and Hanni M. Fakhoury, San Francisco, California, for Amicus Curiae Electronic Frontier Foundation.

PRESENT: Reiber, C.J., Dooley, Johnson, Skoglund and Burgess, JJ.

¶ 1. **DOOLEY, J.** In this complaint for extraordinary relief, we are asked to determine whether a judicial officer has discretion to attach ex ante or prospective conditions to a search warrant. The State petitions this Court to strike ten such conditions pertaining to the search of a personal computer, seized by police as part of an identity theft investigation. The State contends that the conditions exceed the judicial officer's authority under the Fourth Amendment and unnecessarily impede law enforcement's ability to investigate crime. Two amici have filed briefs in opposition to the State's petition, and they argue that the conditions are a valid exercise of the judicial officer's authority and are necessary to protect personal privacy. We grant the petition in part and strike the condition abrogating the plain view doctrine. Because we conclude that the remaining conditions serve legitimate privacy interests, the petition is otherwise denied.

¶ 2. In December 2010, a Burlington Police Detective was assigned to investigate an identity

theft case transferred from the New York State Police. In conjunction with the investigation, he applied for a warrant to search a home at [Address Omitted] in Burlington. The affidavit submitted in support of the warrant recites the following facts.

¶ 3. The crime was reported by a resident of New York. In an interview with the Vermont detective, the victim stated that someone had fraudulently attempted to apply for credit cards online using his name and identifying information and to change his address with the United States Postal Service. Based on this information, the detective contacted one of the banks involved and obtained the internet protocol (IP)[1] address that was used to submit one of the fraudulent credit card applications. The bank also provided the information submitted in the online application, which listed the victim's true name and social security number, but contained other information that was false, including an address of [Address Omitted], Burlington, Vermont, and an electronic mail address of gulfields@aol.com. Both police and motor vehicle records indicate that [Address Omitted] is occupied by Eric Gulfield.

---

[1] As defined in the detective's affidavit, an IP address is a unique numeric series assigned to each computer connected to the internet. It specifically identifies that computer so that internet traffic may be properly directed to and from that computer. *See Kleffman v. Vonage Holdings Corp.,* 232 P.3d 625, 627 (Cal. 2010) (defining IP address).

¶ 4. From the internet service provider, the detective learned that at the time the fraudulent application was submitted online, the IP address used belonged to a subscriber listed at [Address Omitted]. The detective visited the location and observed that there was an open (unprotected by a password) wireless internet (WIFI) connection coming from [Address Omitted]. He determined that the signal was likely strong enough to access from [Address Omitted]. The detective interviewed the resident of [Address Omitted] and obtained permission to access the router log to determine if other computers had used the wireless connection. From this log, the detective discovered that the previous month the router was accessed several times by a computer with an assigned name of GulfieldProp-PC.

¶ 5. Based on the foregoing information, the detective applied for a warrant to search [Address Omitted] for "evidence of the crime of Identity Theft." The application requested permission to seize records "in whatever form they are found," including any computers or other electronic medium. An attachment described the property to be seized in more detail, including:

> Any computers or electronic media, including hard disks, magnetic tapes, compact disks ("CD"), digital video disks ("DVD"), cell phones or mobile devices and removable storage devices such as thumb drives, flash drives, secure digital ("SD") cards or similar

> devices, floppy disks and zip disks (hereinafter "MEDIA") that were or may have been used as a means to commit the offense described on the warrant.

The application did not list one person as the target of the search; rather, it noted that multiple people were living in the target address and requested permission to seize electronic devices regardless of ownership. As justification, the affidavit explained that electronic information may be easily moved between different computers and other electronic storage devices.

¶ 6. Reciting general information about the large volume of information stored on a computer, the technical expertise required to search data that can be hidden, password protected, or encrypted, and the time involved in such a search, the application requested authorization to seize any computers for search off-site. The application further stated:

> 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. In light of these difficulties, the [applicant] intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence. . . .

¶ 7. The judicial officer reviewing the request granted a warrant to search the residence and to seize electronic devices to be searched at an off-site facility for as long as reasonably necessary. In a separate order, however, the judicial officer stated only that "[t]he application to search the computer belonging to Eric Gulfield is *granted,*" and attached conditions: (1) restricting the police from relying on the plain view doctrine to seize any incriminatory electronic record not authorized by the warrant – that is, "any digital evidence relating to criminal matters other than identity theft offenses"; (2) requiring third parties or specially trained computer personnel to conduct the search behind a "firewall" and provide to State investigatory agents only "digital evidence relating to identity theft offenses"[2]; (3) requiring

[2] We interpret this restriction to mean that the person(s) conducting the search may provide digital evidence relating to

(Continued on following page)

digital evidence relating to the offenses to be segregated and redacted from surrounding non-evidentiary data before being delivered to the case investigators, "no matter how intermingled it is"; (4) precluding State police personnel who are involved in conducting the search under condition (2) from disclosing their work to prosecutors or investigators; (5) limiting the search protocol to methods designed to uncover only information for which the State has probable cause; (6) precluding the use of specialized "hashing tools" and "similar search tools" without specific authorization of the court; (7) allowing only evidence "relevant to the targeted alleged activities" to be copied to provide to State agents; (8) requiring the State to return "non-responsive data" and to inform the court of this action; (9) directing police to destroy remaining copies of electronic data absent judicial authorization otherwise; and (10) requiring the State to file a return within the time limit of the warrant[3] to indicate precisely what data was obtained, returned, and destroyed. Law enforcement conducted a search of the premises and seized, but did not search, a personal computer and an iPad.[4]

---

any identity theft offenses, not only that involving the specific identified New York victim.

[3] In this case, the warrant authorized the police to take "as long as reasonably necessary" to search the items seized.

[4] According to the State, the computer was imaged and subsequently returned; however, because the iPad could not be imaged it has been retained by the Burlington Police Department. It is unclear whether the iPad is included in the phrase "the

(Continued on following page)

¶ 8. The State then filed a motion for extraordinary relief in this Court requesting that the Court strike the ex ante conditions from the warrant. In support of its petition, the State argues that the judicial officer lacked authority to impose ex ante restrictions on the search; that the conditions are unnecessary and impede legal development in the area of computer searches; and that the conditions impermissibly impede effective law enforcement investigation. The Defender General and the American Civil Liberties Union (ACLU)[5] submitted briefs as amici curiae in opposition to the State's petition.[6] The ACLU argues that computers are fundamentally different from paper records or filing cabinets because of the vast volume of personal data stored in a computer and due to a computer's unique ability to retain hidden and deleted information and to act as a portal to other remote storages of information. To protect privacy, the ACLU argues that the Fourth Amendment demands more stringent requirements to search electronic devices. The Defender General argues that

---

computer belonging to Eric Gulfield" in the order, and neither side has addressed the iPad in the presentations to this Court. Accordingly, we have not specifically addressed the iPad.

[5] The amicus brief referred to herein as the ACLU brief was submitted on behalf of three organizations: the ACLU Foundation, the ACLU Foundation of Vermont, and the Electronic Frontier Foundation.

[6] Because the investigation is ongoing, no charges have been filed in this case and thus there is no defendant to oppose the State's petition.

such conditions are key to protecting privacy under Article 11 of the Vermont Constitution. Therefore, both amici contend that the conditions are necessary and not beyond the judge's discretion in issuing a warrant.

I.

¶ 9. We first must address the jurisdictional grounds for this action. This is an original jurisdiction case instigated by the State's direct petition for extraordinary relief. Extraordinary relief is a "flexible procedure" that is available when all other avenues are closed. *In re Vt. Sup. Ct. Admin. Directive No. 17,* 154 Vt. 392, 397, 579 A.2d 1036, 1039 (1990). Extraordinary relief is, however, limited to when "there is no adequate remedy by appeal" or by filing for extraordinary relief in the superior court. V.R.A.P. 21(b). In this case, there is no remedy by appeal because the State has no right of appeal from a judge's decision to grant, but condition, a warrant request. *See* 13 V.S.A. § 7403 (limiting State's ability to appeal in criminal cases to situations where prosecution has begun). The State argued that this is a rare case where extraordinary relief is appropriately brought in this Court in the first instance because the issue raised is a pure question of law that requires no factual development. *Cf. In re Hill,* 149 Vt. 86, 86, 539 A.2d 992, 993 (1987) (per curiam) (dismissing petition for extraordinary relief where issues could be dealt with in the course of litigation and on appeal if necessary).

¶ 10. The Defender General moved to dismiss the petition for lack of jurisdiction, arguing that there was no live controversy because the State's contention of injury was speculative and that there were other available means for relief. The Defender General contended that the State should file its petition for extraordinary relief in the civil division in the first instance for further factual development. This Court denied the motion. We now reaffirm that denial. The petition for relief may be decided by this Court in the first instance given that the State is challenging the judicial officer's authority to impose the conditions, as in the nature of a mandamus action, which is a purely legal question that requires no evidentiary analysis. *See*, *e.g.*, *State v. Saari,* 152 Vt. 510, 514-15, 568 A.2d 344, 347 (1989).

¶ 11. Although we conclude that there is jurisdiction, we also emphasize that extraordinary relief in the nature of mandamus is a limited remedy. It is to be granted only when the State shows that the judge's decisions "were usurpations of judicial power, *clear* abuses of discretion, or arbitrary abuses of power." *State v. Pratt,* 173 Vt. 562, 563, 795 A.2d 1148, 1149 (2002) (mem.). Therefore, we must determine whether the judicial officer's decision to impose ex ante restrictions was an abuse of power, clearly contrary to law.

II.

¶ 12. Having found jurisdiction, we consider the scope of this appeal. The central premise of the judicial officer who issued the warrant, a premise reiterated by amici, is that the State is bound by the warrant conditions, hereinafter referred to as instructions. In general, this is settled law: warrant instructions are binding so that a violation of them renders the search unconstitutional. *United States v. Brunette,* 76 F. Supp. 2d 30, 42 (D. Me. 1999) ("It is settled law that the search and seizure of evidence, conducted under a warrant, must conform to the requirements of that warrant."). Enforcing an issuing judicial officer's directions ensures that the warrant requirement is meaningful and effective. *See United States v. Leon,* 468 U.S. 897, 914 (1984) ("[T]he preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination." (quoting *Spinelli v. United States,* 393 U.S. 410, 419 (1969))). Thus, for example, a failure to abide by the warrant's time restrictions may be cause for suppression of evidence obtained in the search pursuant to the warrant. *See Sgro v. United States,* 287 U.S. 206, 211 (1932); *United States v. Bedford,* 519 F.2d 650, 655 (3d Cir. 1975) ("If the police were allowed to execute the warrant at leisure, the safeguard of judicial control over the search which the fourth amendment is intended to accomplish would be eviscerated.").

¶ 13. The State argues, however, that this settled law does not apply to ex ante instructions –

that is, instructions imposed with the warrant on how to execute the warrant. The instructions in this case are ex ante instructions. Essentially, the State's position is that the requirements of the Fourth Amendment of the Federal Constitution and Chapter I, Article 11 of the Vermont Constitution do not extend to such instructions so that violation of these instructions would not itself make the search unconstitutional.[7] Secondarily, the State argues that the judicial officer does not have the power to issue such instructions under Vermont law so they are invalid irrespective of the constitutional mandate.

¶ 14. The issues in this case are unlike the search and seizure questions that we have resolved in the past. The difference involves the nature of the constitutional guarantee, as a right of a citizen to be free from a search and/or seizure that does not comport with constitutional requirements. In the usual case, a criminal defendant argues that certain evidence to be used by the State was obtained in violation of the constitutional mandate and cannot be used against defendant in the criminal proceeding. Here, the issue is whether the judicial officer in approving a

[7] The State phrases its argument in different ways. It has briefed them under the general heading that the magistrate exceeded his authority in issuing the instructions. Neither the Federal nor the Vermont Constitution purports to regulate whether a judicial officer can issue binding instructions on how a search can be conducted. Phrased this way, the question is one of Vermont non-constitutional law. We have rephrased the question consistent with the substance of the State's argument.

search warrant can add instructions to protect the privacy interests of the person to be searched. The issue has never been addressed directly by the U.S. Supreme Court and has rarely been addressed by lower federal courts or courts in other states.

¶ 15. While the State has argued briefly that Article 11 creates no greater power to issue ex ante instructions as part of the constitutional mandate, and the Defender General argues to the contrary urging us to ground our decision on the Vermont Constitution, this case is fundamentally about the reach of the Fourth Amendment. The judicial officer relied upon Fourth Amendment decisions in imposing the instructions, and the parties have relied upon Fourth Amendment decisions in their arguments to this Court. In part, this is because there are no state constitution precedents. To be sure, we have noted on many occasions that Article 11 "may offer protections beyond those provided by the Fourth Amendment," *State v. Roberts,* 160 Vt. 385, 392, 631 A.2d 835, 840 (1993), and this case could involve a variation of this principle. Our first impression, however, is that this case is less about the scope of protections of a constitutional provision and more about the tools available to ensure that protection occurs. Thus, any holding we might ultimately make concerning the scope of Article 11 with respect to ex ante instructions will be based on a new analysis of the protections of that Article. In view of our disposition of the case under the Fourth Amendment, we decline to engage in such an analysis in this case.

¶ 16. Nor do we rest our decision on Vermont non-constitutional law. While the State argued that Vermont law does not authorize a judicial officer to impose ex ante instructions, it addressed only Vermont Rule of Criminal Procedure 41. It argued that this criminal procedure rule does not authorize the magistrate to issue instructions on how the search shall be conducted. Although Rule 41 is relevant,[8]

[8] More relevant is 24 V.S.A. § 293, which addresses the powers and responsibilities of a sheriff, and by cross-reference all other law enforcement officers in Vermont. The statute was enacted in 1787 and has stood since then essentially without amendment, as seen in the history noted following the statute. The statute provides that the sheriff "shall serve and execute lawful writs, warrants and processes directed to him, *according to the precept thereof.*" *Id.* (emphasis added). A precept in this context is a warrant "issued by an authorized person demanding another's action." Black's Law Dictionary 1215 (8th ed. 2004). We take it to mean the command – as opposed to the authorization – contained in a warrant; in other words, it is the magistrate's instruction. The construction issue raised by § 293 is whether the ex ante search instructions represent a valid precept, essentially as understood from the Vermont common law.

There is currently no statutory law on the power of the issuing magistrate. Early statutes referred the question back to the common law. Thus, the law as compiled in the Revised Statutes of 1840 stated that "Justices [of the Peace] may issue all writs, warrants and precepts, necessary to carry into effect the powers granted to them, and where no form therefor is prescribed by statute, they shall frame one in conformity with the principles of law and the usual course of proceedings of courts in this state." R.S. Ch. 26, § 61. Although the Legislature provided many forms for writs and precepts, it never provided one for a search warrant. Henry Harmon in his treatise on the Common Law and Equity Procedure suggests a form for a

(Continued on following page)

neither it, nor the federal rule on which it is based, purport to completely define the scope of judicial power with respect to search warrants. Thus, we are not persuaded on this limited record that Vermont law supports the State's argument and do not consider it further.

¶ 17. Before addressing the substantive claims of error raised, we briefly make three points that put our analysis in context and respond to one of the points made by the dissent. First, there are really two searches in this case – the first for the computer and the second of the computer. The first has occurred and is not in dispute; the issues relate solely to the second search. Second, the principal question before us is whether the warrant-issuing magistrate had the authority to issue the specific search instructions he did, not as the dissent suggests, whether imposing the instructions is necessary to comply with the Fourth Amendment or Chapter I, Article 11 of the Vermont Constitution. Third, the State has challenged the imposition (or effect) of the instructions in general. Assuming such instructions could be imposed and they are binding under either the federal or state constitution, the State has not argued that they were

---

warrant to enter a dwelling house to search for stolen goods. H. Harman, *The Principles of Common Law and Equity Procedure: A Manual of Court Procedure* § 163 (1912). The warrant specifies that if the sheriff finds the described property, he shall "bring the said [goods and chattels] so found, forthwith before me at [my office]." This appears to be a form of ex ante precept.

inappropriate in this case. We leave questions about the nature and extent of the magistrate's discretion in this area to another day.

III.

¶ 18. We now proceed to the main question before us – whether a judicial officer issuing a warrant has the authority to place ex ante instructions on how a search may be conducted. We have stated the question broadly because the State has challenged the authority of the judicial officer to impose any ex ante instructions, not particularly those in this case.[9] We also emphasize that the general question is one of authority, and not responsibility. No party or amicus is directly claiming that ex ante instructions are ever required, and we certainly do not hold so here.

¶ 19. Under the Fourth Amendment, people are protected "against unreasonable searches and seizures." U.S. Const. amend. IV. This right is echoed in the Vermont Constitution, which protects people's right to be "free from search or seizure." Vt. Const. ch. I, art. 11. "Absent exceptional circumstances, the federal and state constitutions instruct executive officers to conduct searches pursuant to a warrant issued by an impartial magistrate." *State v. Quigley,*

[9] The State does argue that certain of the instructions are inappropriate, and we have addressed these arguments after consideration of the main question.

2005 VT 128, ¶ 11, 179 Vt. 567, 892 A.2d 211. Warrants may not be granted "but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV; *see* Vt. Const. ch. I, art. 11 (requiring that warrants be supported by a "sufficient foundation" and with the items to be seized "particularly described"); *see also United States v. Wuagneux,* 683 F.2d 1343, 1349 (11th Cir. 1982) (interpreting particularity requirement to mean that "a description of property will be acceptable if it is as specific as the circumstances and nature of the activity under investigation permit"). As we set out above, this case poses the question of whether a judicial officer – in carrying out his or her role of safeguarding these Fourth Amendment and Article 11 rights – may include certain ex ante instructions in a search warrant such that violation of the instructions will make the search unconstitutional.

¶ 20. In creating the instructions, the issuing judicial officer explicitly relied on *United States v. Comprehensive Drug Testing, Inc. (CDT I),* 579 F.3d 989 (9th Cir. 2009) (en banc). That case arose out of a 2002 federal investigation into the Bay Area Lab Cooperative (Balco), which the government suspected of providing illegal steroids to professional baseball players. That year, Major League Baseball and the Player's Association agreed to test all players to determine if more than five percent of players tested positive for steroid use. Under the agreement, the

results of the testing of individual players were to be kept confidential. The samples were collected by an independent business, Comprehensive Drug Testing, Inc. (CDT), and the tests were performed by a private laboratory, Quest Diagnostics, Inc. CDT retained the list of players and their respective test results while Quest kept the specimens.

¶ 21. As part of its Balco investigation, the government developed probable cause to believe ten players tested positive for steroids. The government secured a grand jury subpoena to obtain all drug testing records and specimens in CDT's possession. The players moved to quash this subpoena. The government also obtained a warrant authorizing a search of CDT. Although the warrant was limited to the records of the ten players for whom the government had probable cause, when the government executed the warrant, law enforcement seized and reviewed the drug testing records for hundreds of baseball players as well as other individuals. Litigation ensued challenging the government's action. CDT and the players moved for return of property under Federal Rule of Criminal Procedure 41(g), and the players moved to quash the subpoena.

¶ 22. The motions were heard by three different district court judges who all ruled against the government, granting the motions to return property and quashing the subpoena. All "expressed grave dissatisfaction with the government's handling of the investigation." *Id.* at 994. On appeal, a panel of the United States Court of Appeals for the Ninth Circuit reversed

two decisions, concluding that the government's seizure did not violate the law. *United States v. Comprehensive Drug Testing Inc.,* 473 F.3d 915 (9th Cir. 2006). The court then granted a rehearing en banc[10] and upheld the district court orders, finding against the government. Following its detailed analysis of the case, the court included some "Concluding Thoughts" regarding the challenge of balancing law enforcement's need "for broad authorization to examine electronic records" with the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *CDT I,* 579 F.3d at 1004. Noting that it was best "if there are clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment," the court outlined a list of "guidance" for magistrates to employ when issuing warrants for search of electronic devices. *Id.* at 1006. This included: insisting the government waive reliance on the plain view doctrine; requiring segregation or redaction of data by an independent third party prior to release to investigators; requiring the government to use a search protocol designed to uncover only information for which there is probable cause; and mandating that the government destroy or return nonresponsive data. *Id.*

---

[10] The en banc decision was issued by a court of nine judges, roughly half of those on the court.

CDT I emphasized the need for such restrictions to prevent government overreaching, as had occurred in that case, and to protect the privacy interests of third parties.

¶ 23. Dissatisfied, the government then moved for review by all twenty-one active judges of the Ninth Circuit, arguing that the search protocols announced in the decision were unnecessary to resolve the case, beyond the court's authority, and harmful to ongoing government investigations. Brief for the United States in Support of Rehearing En Banc by the Full Court, *CDT I,* 579 F.3d 989 (9th Cir. 2009) (Nos. 05-10067, 05-15006, 05-55354). In response, the initial en banc decision was revised and replaced with *United States v. Comprehensive Drug Testing, Inc. (CDT II),* 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam). While the revised decision retained the substantive analysis and legal outcome of *CDT I,* the guidelines were removed from the per curiam opinion, and instead were included in a concurrence. *CDT II,* 621 F.3d at 1180 (Kozinski, C.J., concurring). The instructions adopted by the judicial officer in this case are drawn from the guidelines that were set forth in *CDT I* and retained only in the concurring opinion in *CDT II*.

¶ 24. The State contends that the judicial officer in this case lacked authority to impose the instructions at issue. In the State's view, rather than authorizing a search at a particular location or for particular items, the judicial officer was attempting to dictate *how* law enforcement must conduct its

search. In making this argument, the State draws heavily on an article written by Professor Orin Kerr following *CDT I. See* O. Kerr, *Ex Ante Regulation of Computer Search and Seizure,* 96 Va. L. Rev. 1241, 1242 (2010). Professor Kerr argues that "ex ante restrictions on the execution of computer search warrants are constitutionally unauthorized and unwise." *Id.* He contends that ex ante restrictions are impermissible because they predetermine the reasonableness of a search – a matter that he contends is beyond a magistrate's authority under the Fourth Amendment.[11] According to this view, an issuing

[11] In support, Professor Kerr relies on four Supreme Court decisions that he claims demonstrate that magistrates do not have authority to dictate how a reasonable search must be conducted and any attempt to do so will have no effect. *United States v. Grubbs,* 547 U.S. 90, 97 (2006) (concluding that Fourth Amendment does not require triggering condition for anticipatory warrant be particularly described because constitution "does not set forth some general 'particularity requirement' "); *Richards v. Wisconsin,* 520 U.S. 385, 395 (1997) (affirming ability of magistrate to issue no-knock warrant, but holding that no-knock entry was reasonable under circumstances even when warrant for such was not granted in advance); *Lo-Ji Sales, Inc. v. New York,* 442 U.S. 319, 326-27 (1979) (holding that magistrate's participation in search of adult bookstore to determine if materials were obscene violated Fourth Amendment's requirement of neutral and detached magistrate); *Dalia v. United States,* 441 U.S. 238, 256-57 (1979) (concluding wiretap warrant need not include specific authorization to enter target premises because "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"). As discussed more fully below, we do not view these cases as supporting the conclusion drawn by Professor Kerr. What they do support are two more modest

(Continued on following page)

officer's role is only to determine whether probable cause exists to search a given location, not to determine the manner in which a search may be conducted. Drawing on Professor Kerr's argument, the State contends that the judicial officer exceeded the narrowly circumscribed role of an officer reviewing a warrant application and, thus, its instructions are not part of the constitutional mandate.

¶ 25. The permissibility of imposing the ex ante instructions on computer searches is a relatively novel question for courts generally.[12] What tools are at

---

conclusions: that ex ante evaluation by a judicial officer cannot wholly supplant ex post assessment of law enforcement conduct and that hard and fast rules about what a warrant must and must not include are generally frowned upon.

[12] While some courts have addressed whether certain ex ante parameters are *required,* few courts have addressed whether such conditions are a *permissible* exercise of authority. *See In re Search of 3817 W. West End,* 321 F. Supp. 2d 953, 957 (N.D. Ill. 2004) ("[W]hen deciding to issue a warrant that would involve the seizure and subsequent search of a home computer, a magistrate judge has the authority to require the government to set forth a search protocol that attempts to ensure that the search will not exceed constitutional bounds."). In advocating for their advisability, the per curiam opinion in *CDT I* and the concurring opinion in *CDT II* clearly presuppose that such conditions may permissibly be imposed, but the court never directly addressed the challenge raised by Professor Kerr's article and by the State's brief. Several commentators have advocated for the use of ex ante conditions in computer searches. *See, e.g.*, S. Brenner & B. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues,* 8 Mich. Telecomm. & Tech. L. Rev. 39, 82-84 (2002) (advocating the use of search protocols for computer warrants); R. Winick, *Searches and Seizures of*

(Continued on following page)

the disposal of judicial officers in confronting the challenges presented by searches of electronic media is a real and important question. As one court succinctly put it: "Computers are simultaneously file cabinets (with millions of files) and locked desk drawers; they can be repositories of innocent and deeply personal information, but also of evidence of crimes. The former must be protected, the latter discovered." *United States v. Adjani,* 452 F.3d 1140, 1152 (9th Cir. 2006). We are not called upon to decide today how these conflicting goals are best satisfied. Our question is not whether the judicial officer's attempt to reconcile these objectives was recommendable, much less required. Our question is simply whether this attempt was such a clear abuse of authority as to merit our prohibition in the context of this petition for extraordinary relief.

¶ 26. In this light, we reject the State's invitation to hold that all ex ante restrictions on the execution of a search warrant are universally of no effect in defining the constitutional requirement. Although the historical record is sparse at this point, we see no bright line that allows some conditions, but not ones that specify how law enforcement officials must conduct their search. Indeed, the evidence from Vermont suggests that such ex ante instructions have been used in the past. *See* discussion *supra* note 8.

Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 102-14 (1994) (encouraging the use of search protocols to regulate computer searches and seizures).

¶ 27. We conclude that ex ante instructions are sometimes acceptable mechanisms for ensuring the particularity of a search. According to Professor Kerr's argument, which the State would have us adopt, a judicial officer's only concern ex ante should be with probable cause and particularity, not reasonableness. Kerr, *supra,* at 1290-91 ("[E]x ante assessment of probable cause and particularity serves a different function than ex ante assessment of how a search should be executed."). Accepting arguendo that such a bright dividing line exists, ex ante instructions may be a way to ensure particularity. Even in traditional contexts, a judicial officer may restrict a search to only a portion of what was requested – a room rather than an entire house, or boxes with certain labels rather than an entire warehouse. In other words, some ex ante constraints – of the form "here, not there" – are perfectly acceptable. Warrant applications describing the proposed scope of a search are not submitted to the court on a take it or leave it basis.

¶ 28. Often the way to specify particular objects or spaces will not be by describing their physical coordinates but by describing how to locate them. This is especially true in the world of electronic information, where physical notions of particularity are metaphorical at best. *Cf.* J. Goldfoot, *The Physical Computer and the Fourth Amendment,* 16 Berkeley J. Crim. L. 112, 123-24 (2011) ("The initial decision to treat storage media as having subcontainers departs from physical moorings; after that departure, metaphors

are necessary to apply physical rules to the new virtual world."). Although the details of computer searches are new and evolving, the need for a non-physical concept of particularity is one that courts have already confronted. Warrants for electronic surveillance routinely set out "minimization" requirements – procedures for how and under what conditions the electronic surveillance may be conducted – in order to "afford[ ] similar protections to those that are present in the use of conventional warrants authorizing the seizure of tangible evidence." *Berger v. New York,* 388 U.S. 41, 57 (1967); *see, e.g.*, *Ricks v. State,* 537 A.2d 612, 621 (Md. 1988) (describing specific minimization procedures such as when camera should be turned on and off and what could and could not be recorded in 22-page order granting warrant for video surveillance).

¶ 29. At this point, many jurisdictions have adopted statutes that not only permit, but require, that warrants for electronic surveillance include procedures for minimizing the capture of non-pertinent information. *See, e.g*., N.Y. Crim. Pro. Law § 700.30 (requiring that warrants contain "[a] provision that the authorization to intercept or conduct video surveillance . . . shall be conducted in such a way as to minimize the interception of communications or the making of observations not otherwise subject to eavesdropping or video surveillance").[13]

[13] Because of debate over applying contemporary Fourth Amendment analysis to computer searches, some have suggested

(Continued on following page)

These provisions in the warrants are ex ante conditions on how a search may be conducted, but we believe that they are well within the scope of a judicial officer's role in ensuring that searches are targeted with sufficient particularity. The same reasoning applies with even more force in the computer context. In the digital universe, particular information is not accessed through corridors and drawers, but through commands and queries. As a result, in many cases, the only feasible way to specify a particular "region" of the computer will be by specifying how to search. We view such ex ante specification as an acceptable way to determine particularity.

¶ 30. Further, we do not agree that one can draw a categorical line between the probable cause inquiry and considerations of privacy. Professor Kerr's argument suggests that consideration of the privacy interests of the person to be searched is ultimately irrelevant to a judicial officer issuing a warrant. *See* Kerr, *supra,* at 1290-92. But this picture is overly rigid, ignoring the fact that the relevant ex ante standards depend on the severity of the privacy

---

that Congress address the issue through legislation. *See, e.g.*, Goldfoot, *supra,* at 161 (noting that policy concerns of computer searches could be addressed through legislative rules like the specialized rules for wiretaps); E. Silbert & B. Chilton, *(Giga)bit by (Giga)bit: Technology's Potential Erosion of the Fourth Amendment,* Crim. Just., Spring 2010, at 4, 11; K. Nakamaru, Note, *Mining for Manny: Electronic Search and Seizure in the Aftermath of United States v. Comprehensive Drug Testing,* 44 Loy. L.A. L. Rev. 771, 801-04 (2011).

infringement that is contemplated. A judicial officer might authorize a search of a person, including his pockets, without any particular basis for thinking that evidence will be found in the person's pocket as opposed to elsewhere on his person. But that same officer might permissibly refuse to authorize a search of the person's body cavities based on evidence of similar generality. *See, e.g.*, *United States v. Nelson,* 36 F.3d 758, 760 (8th Cir. 1994) (holding that probable cause to search defendant's "person" did not include probable cause to perform a body cavity search and that this case clearly exhibits "[t]he need to provide specificity in a warrant"). This is not because a person's rectal cavity is, in any meaningful sense, a more "particular" or "specific" location than his left pocket,[14] but because concerns for privacy inflect our understanding of probable cause and particularity.[15]

---

[14] Although illustrative, intense invasions of bodily privacy are not essential to the point. A judicial officer might plausibly demand that a handbag be described particularly and yet not demand particularity as to which acre of an open field is to be searched. Particularity is not defined in purely physical terms but in terms of how human behavior delineates zones of privacy.

[15] This is a correlate of the accepted proposition that particularity and reasonableness are functionally related. *See, e.g*, *United States v. Burgess,* 576 F.3d 1078, 1094 (10th Cir. 2009) ("A warrant may permit only the search of particularly described places and only particularly described things may be seized. As the description of such places and things becomes more general, the method by which the search is executed

(Continued on following page)

¶ 31. What we ask judicial officers to ensure, therefore, is not simply that there is a reason to believe evidence may be uncovered but that there is a reason that will justify an intrusion on a citizen's privacy interest. The investigatory promise must justify the collateral exposure. *See State v. Savva,* 159 Vt. 75, 86, 616 A.2d 774, 780 (1991) ("Although criminal defendants may seek court review of searches and seizures, these after-the-fact challenges do not serve Article 11's purpose of protecting the rights of everyone – law-abiding as well as criminal – by involving judicial oversight *before* would-be invasions of privacy." (emphasis added)). It is therefore essential that a judicial officer be cognizant of the general type of invasion being proposed. Where the invasion is less, a judicial officer may be more willing to issue the warrant.

¶ 32. As a corollary, judicial officers may describe in general terms what sort of an invasion is authorized. *See United States v. Banks,* 540 U.S. 31, 36 (2003) ("[A] magistrate judge is acting within the Constitution to authorize a 'no-knock' entry."); V.R.Cr.P. 41(c) (requiring that warrants "shall command the officer to search[ ] within a specified period of time"; that they shall be executed during the daytime "unless the warrant directs that it may be served at any time"; and that they shall "designate

---

becomes more important – the search method must be tailored to meet allowed ends. And those limits must be functional.").

the court to which it shall be returned"); *cf. Scott v. United States,* 436 U.S. 128, 130 (1978) (contemplating "judicial authorization which required . . . minimization" of wiretap under 18 U.S.C. § 2518). To say this is not to deny that the ex ante perspective of the issuing officer is to some extent limited. Judicial officers should not micromanage the execution of the warrant. *See Lo-Ji Sales,* 442 U.S. at 326-27. And because the ex ante assessment is general, it will not foreclose ex post reassessment insofar as "the Magistrate could not have anticipated in every particular the circumstances that would confront the officers." *Richards,* 520 U.S. at 396.[16]

¶ 33. It is a serious error, however, to infer from the fact that we must often evaluate ex post whether a search sufficiently respected a citizen's privacy to the conclusion that we can make no ex ante judgments about what sort of privacy invasions are and

[16] One argument advanced both in the State's brief and in Professor Kerr's article is the idea that allowing ex ante restrictions will prevent the evolution of the law. *See* Kerr, *supra,* at 1293 ("[E]x ante restrictions prevent the development of ex post rules of reasonableness that appellate courts must create to account for the new environment of computer search and seizure."). Given that ex post review is not foreclosed, and we are not imposing a requirement that a judicial officer issue any ex ante requirements, we see little reason to accept the premise of this argument. But even if this were not true, we are not persuaded that setting ground rules prior to a search is inferior to raising them after the search was conducted in the context of a request to suppress relevant evidence. As this case demonstrates, review of the ex ante conditions is available.

are not warranted. There is interplay between probable cause, particularity, and reasonableness that judicial officers reviewing a warrant application must consider in authorizing a form of privacy invasion. We therefore reject any blanket prohibition on ex ante search warrant instructions.

IV.

¶ 34. Having rejected a categorical prohibition on ex ante instructions, we examine the specific instructions imposed by the judicial officer in this case and consider whether each was an abuse of authority. For clarity in our analysis, we group the instructions into the following categories: the first – instruction (1) relating to the plain view doctrine; the second – instructions (2), (3), and (4) requiring that the search be performed by third parties or police personnel segregated from the investigators and requiring that the information be segregated and redacted prior to disclosure; the third – instructions (5) and (6) requiring police to use focused search techniques and prohibiting the use of specialized search tools without prior court authorization; and the fourth – instructions (7), (8), (9), and (10) pertaining to the copying, destruction and return of data. We address each of these categories in turn.

A.

¶ 35. First, we consider instruction (1) related to the plain view doctrine. Generally, only the items

specifically described in a search warrant may be seized by law enforcement officers. Under the plain view doctrine, however, "if police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if officers have a lawful right of access to the object, they may seize it without a warrant." *Minnesota v. Dickerson,* 508 U.S. 366, 375 (1993); *see State v. Trudeau,* 165 Vt. 355, 358, 683 A.2d 725, 727 (1996) (listing and applying requirements for plain view doctrine). This applies to items viewed during a warranted search. Thus, when law enforcement is conducting a search pursuant to a warrant, police are authorized to seize objects not listed in the warrant as long as the object is viewed from a lawful vantage point, the incriminating nature of the object is obvious, and it may be seized from a lawful right of access. *Horton v. California,* 496 U.S. 128, 136-37 (1990).

¶ 36. The judge was apparently concerned about how, pursuant to a broad search warrant, the plain view doctrine could be used in this case to seize evidence from computers or other electronic devices that were unconnected to the identity fraud investigation. Therefore, borrowing from *CDT I,*[17] the judge imposed the following instruction:

---

[17] In fact, even the CDT cases do not go as far as recommending abrogation of the plain view doctrine. *CDT I* instructed magistrates to urge the government to waive reliance on plain view, but did not suggest that a magistrate has authority under

(Continued on following page)

> [T]he 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.

The State challenges this instruction on the same basis as all the others – that the court had no authority to delineate *how* law enforcement should conduct the search. Amici argue that it is necessary to abrogate the plain view doctrine in cases involving searches of computers because otherwise the search will transform into a general search violating individuals' privacy interests.[18]

---

the Fourth Amendment to actually preclude the government from seizing an object over which an individual has no privacy interest. *CDT I,* 579 F.3d at 1006.

[18] Amici base their argument on what they deem are certain unique attributes of electronic media, including: the large volume of information contained on electronic devices, especially that of a highly personal nature; the ability to retrieve items the user may not have intended to save or attempted to delete; and the connectivity of electronic devices. *See, e.g.*, *United States v. Flyer,* 633 F.3d 911, 918 (9th Cir. 2011) (explaining how government can retrieve deleted information from unallocated space on computer); *Burgess,* 576 F.3d at 1090 (noting the "unique ability" of electronic devices such as "laptop computers, hard drives, flash drives or even cell phones" to contain "vast amounts of diverse personal information").

¶ 37. For two main reasons, we find this first instruction unnecessary for privacy protection and inappropriate. It is unnecessary because instructions (2), (3) and (4), requiring the segregation of the search from the investigation and limiting the results of the search that can be shared, obviate application of the plain view doctrine. Investigatory personnel will never be in the position to view incriminating evidence unrelated to identity theft offenses.

¶ 38. Second, we conclude that it is beyond the authority of a judicial officer issuing a warrant to abrogate a legal doctrine in this way. "Judicial supervision of the administration of criminal justice in the . . . courts implies the duty of establishing and maintaining civilized standards of procedure and evidence." *McNabb v. United States,* 318 U.S. 332, 340 (1943). This supervisory power does not, however, go so far as to allow a judicial officer to alter what legal principles will or will not apply in a particular case. This proposition was established in *United States v. Payner,* 447 U.S. 727 (1980), in which the trial court attempted to use its supervisory authority to suppress items seized in violation of a third party's constitutional rights, thereby avoiding the established rules for Fourth Amendment standing. In reversing, the Supreme Court concluded that, if it accepted such use of the supervisory power, it "would confer on the judiciary discretionary power to disregard the considered limitations of the law it is charged with enforcing." *Id.* at 737. In this case, allowing instruction (1) would confer on a judicial

officer the authority to pick and choose what legal doctrines would apply to a particular police search. Because we do not believe that a judicial officer holds such authority, we conclude that the State's petition for extraordinary relief must be granted with regard to instruction (1).

B.

¶ 39. Next, we turn to instructions (2), (3), and (4) requiring that the search be performed by third parties or trained computer personnel separate from the investigators and operating behind a firewall. The principal instruction on this topic reads in full:

> 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.

Further, the court directed that if segregated state investigators were used, they could not disclose information other than that related to the "identity theft offenses." If private third parties were employed, the court required them to deliver only "digital evidence relating to the offenses being investigated" and to segregate and redact it from

non-evidentiary data "no matter how intermingled." These instructions are the heart of the court's ex ante order.

¶ 40. Again, the State contends that the judicial officer had no authority to impose these instructions because it was an attempt to dictate *how* law enforcement should reasonably conduct the search. *See* Kerr, *supra,* at 1277. The ACLU argues that the separation and screening instructions are necessary to protect privacy by ensuring that investigations have independent sources and that police objectives do not become comingled. The Defender General contends that the segregation procedures protect privacy by providing "the mechanism to ensure that the State would not gain access to data that it had no probable cause to collect." The Defender General also argues that the standard under the Vermont Constitution is more stringent than its federal counterpart because Article 11 requires that a search be conducted "in the least intrusive manner." *State v. Birchard,* 2010 VT 57, ¶ 13, 188 Vt. 172, 5 A.3d 879.

¶ 41. The application for the warrant in this case requested incredibly broad authorization. The affidavit in support of the search warrant application says that in some cases searching for evidence relevant to the charged crime can involve "carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials." It goes on to say, however, that in other cases these techniques will not yield all the relevant evidence because "[c]riminals 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." The affidavit asserts that the criminal's 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." The affidavit also states that because electronic data can easily be moved to other computers within the house, law enforcement must search all computers, even those belonging to persons not suspected of committing a crime.

¶ 42. In short, the warrant application could not have requested a broader authorization: that is, to search all files in all ways on all computers in the house. *See* P. Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges,* 97 Va. L. Rev. In Brief 1, 11 (2011) ("Computer search warrants are the closest things to general warrants we have confronted in the history of the Republic."). Understandably, in the judicial officer's view, the warrant application did not provide probable cause for such a wide ranging search. *See United States v. Otero,* 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging

search into a person's private affairs, and accordingly makes the particularity requirement that much more important.").

¶ 43. The separation and screening instructions are the judicial officer's attempt to remedy this lack of particularity. To accomplish this, the instructions require that only the particular information for which there is probable cause to search will be laid bare to police investigators. *See Marron v. United States,* 275 U.S. 192, 196 (1927) ("The 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 opposed to exposing the entire contents of the hard drive to the police, the procedures ensure that only those files that relate to the suspected criminal activity will be viewed. In lieu of a particular description of the relevant files, the conditions create a procedure for identifying the relevant files and exposing only them to police investigators.

¶ 44. The State and the dissent raise two general objections to the instructions. The first, particularly raised by the dissent, is that the instructions have improperly eviscerated the plain view doctrine. *Post,* ¶ 84. Although the practical consequences of the instructions may be comparable to an abrogation of the plain view doctrine, the mechanism is critically different. Abrogating the plain view doctrine would mean that investigating police officers could not seize evidence that they incidentally viewed. The screening

procedures, in contrast, prevent such incidental police viewings from ever occurring. It is not an abrogation of the plain view doctrine to put in place safeguards against the police plainly viewing.[19] By separating police investigators and third-party screeners, these instructions – almost by definition – ensure a particularity of the exposure to police while avoiding the abrogation of the plain view doctrine.

¶ 45. In making their argument, the dissent is treating the plain view doctrine as some form of right of law enforcement officials. The dissent refers to "frustrat[ing]" and "interfer[ing] with" the plain view doctrine. *Post,* ¶¶ 84, 100. In fact, the plain view doctrine has a very limited role in Fourth Amendment jurisprudence. It is related only to seizures, not to searches. *Horton,* 496 U.S. at 134 (stating that plain view is an "exception that is addressed to the concerns that are implicated by seizures rather than by searches"). The doctrine itself is concerned with the permissible actions of the investigator after he or she has seen the incriminating evidence, not before. As we said in *State v. Birchard,* the "plain-view doctrine comes into play as an exception only where

[19] Nor, for example, would restrictions on misleading advertising count as abrogating the principle of caveat emptor. Nor, for that matter, would a nursery school putting in place precautions against students losing their belongings be an abrogation of the "finders-keepers" doctrine. In each case, the restrictions don't eliminate the doctrine; they simply attempt to prevent situations calling for its application to arise as frequently.

an officer *has* observed the object in question." 2010 VT 57, ¶ 27, 188 Vt. 172, 5 A.3d 879.

¶ 46. An examination of the U.S. Supreme Court cases that developed the doctrine make it clear that it was crafted to be a narrow exception to the warrant requirement, permissible only as a convenience. The primary development of the doctrine was in the plurality opinion in *Coolidge v. New Hampshire,* which made the practical rational [sic] underlying the doctrine clear: "Where, once an otherwise lawful search is in progress, the police inadvertently come upon a piece of evidence, it would often be a *needless inconvenience,* and sometimes dangerous – to the evidence or to the police themselves – to require them to ignore it until they have obtained a warrant particularly describing it." 403 U.S. 443, 467-68 (1971) (emphasis added). The opinion noted the reasons for the warrant requirement and stated, in part, that allowing the seizure of evidence in plain view without a warrant would not interfere with a primary rationale for the warrant requirement that "those searches deemed necessary should be as limited as possible." *Id.* at 467. It would not do so, the Court found, because the plain view doctrine "does not convert the search into a general or exploratory one."[20] *Id.*

[20] The circumstances here suggest that this characterization may have been optimistic.

¶ 47. Having established the compatibility of the plain view doctrine and the constitutional principles at stake, the plurality found the exception acceptable: "As against the minor peril to Fourth Amendment protections, there is a major gain in effective law enforcement." *Id.* Later cases have recognized the same rationale. *See Dickerson,* 508 U.S. at 375 ("The warrantless seizure of contraband [that officers see in plain view during a valid search] is deemed justified by the realization that resort to a neutral magistrate under such circumstances would often be impracticable and would do little to promote the objectives of the Fourth Amendment."). We have explained the plain view doctrine as an "exception to the warrant requirement." *Trudeau,* 165 Vt. at 358, 683 A.2d at 727.

¶ 48. It is difficult to imagine how we could frustrate a doctrine based on convenience to establish an exception to the warrant requirement. The rationale has nothing to do with a law enforcement officer's access to evidence; it determines only whether the officer must obtain a warrant to seize evidence to which the officer has access. Thus, we cannot accept the argument that the instructions impermissibly abrogate the plain view doctrine.

¶ 49. Second, the State and the dissent argue that allowing the information to be viewed by any third party – even one behind a firewall so the information cannot be viewed by a law enforcement officer – eliminate any legitimate privacy interest. *Post,* ¶ 90. Put another way, the issue, is whether the

conditions meaningfully advance privacy interests in a way that would justify their imposition on the State. Superficially, the answer is not obvious because a citizen's private information is being exposed one way or another, be it to a police officer or a third-party analyst.[21] The police investigators see only the particular files relevant to the investigated crimes, but other files will inevitably be viewed by the screener. If the information exposure is the same

[21] The illusory appeal of this argument – that there is no privacy interest at stake insofar as there will be exposure to someone – may derive in part from an analogy to cases in which one's expectation of privacy is extinguished by voluntary disclosure to a third party. But coerced exposure is altogether different from voluntary disclosure. It is true that, when someone transmits information or places information in public view, that person is often deemed to have abandoned any legitimate expectation of privacy. *See Smith v. Maryland,* 442 U.S. 735, 743-44 (1979) ("This court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). It does not follow, however, that a coerced exposure of information to a third party destroys all legitimate expectations of privacy. *See Fraternal Order of Police v. City of Philadelphia,* 812 F.2d 105, 118 (3d Cir. 1987) ("The fact that protected information must be disclosed to a party who has a particular need for it does not strip the information of its protection against disclosure to those who have no similar need."). Whereas a voluntary exposure involves a person choosing to lower his or her expectation of privacy, a coerced exposure involves no such choice. To hold otherwise would be to conclude that, because the information is going to be exposed to someone contrary to the subject's expectations, the expectation of privacy disappears, and, with it, the constitutional protection. The State cannot bootstrap its way into extinguishing any expectations of privacy because it is justified in trespassing upon that expectation.

either way, one might argue that these instructions ultimately offer no real protection. *See Douglas v. Windham Super. Ct.,* 157 Vt. 34, 39, 597 A.2d 774, 777 (1991) (explaining that this Court will grant a motion for extraordinary relief if, but only if, there is no ground for the trial court's action).

¶ 50. What this argument fails to recognize, however, is that privacy concerns not only our interest in determining *whether* personal information is revealed to another person but also our interest in determining *to whom* such information is revealed. A more complex understanding of privacy – one not limited to mere concern with avoiding exposure altogether – will inevitably acknowledge that our interest in privacy is, at least in part, an interest in to whom information concerning us is exposed. *See Nat'l Cable & Telecomms. Ass'n v. FCC,* 555 F.3d 996, 1001 (D.C. Cir. 2009) ("It is widely accepted that privacy deals with determining for oneself when, how and to whom personal information will be disclosed to others."); *Stone v. State Farm Mut. Auto. Ins. Co.,* 185 P.3d 150, 155 (Colo. 2008) ("[Privacy] includes 'the power to control what we shall reveal about our intimate selves, to whom, and for what purpose.'" (quoting *Martinelli v. Dist. Ct. ex rel. City & Cnty of Denver,* 612 P.2d 1083, 1091 (Colo. 1980))); C. Fried, *Privacy,* 77 Yale L.J. 475, 482 (1968) ("It is not true, for instance, that the less that is known about us the more privacy we have. Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information

about ourselves."); K. Karst, "*The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data,* 31 Law & Contemp. Probs. 342, 344 (1966) ("Meaningful discussion of privacy . . . requires the recognition that ordinarily we deal not with an interest in total nondisclosure but with an interest in selective disclosure."); R. Parker, *A Definition of Privacy,* 27 Rutgers L. Rev. 275, 281 (1974) ("[P]rivacy is control over when and by whom the various parts of us can be sensed by others."); D. Solove, *Conceptualizing Privacy,* 90 Cal. L. Rev. 1087, 1108-09 (2002) ("[E]quating privacy with secrecy . . . fails to recognize that individuals want to keep things private from some people but not others. . . . Secrecy as the common denominator of privacy makes the conception of privacy too narrow."). In short, all exposures are not created equal.[22]

---

[22] The United States Supreme Court has itself acknowledged the inadequacy of the contrary conception of privacy. In *United States Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749 (1989), the Court held that disclosure of FBI rap sheets in response to a Freedom of Information Act request could constitute an unwarranted invasion of personal privacy despite the fact that the information in the rap sheets had been publicly disclosed previously. The Court recognized that "there are few facts that are not at one time or another divulged to another," and that privacy often depends on "the degree of dissemination." *Id.* at 763. The Court then stated, "Recognition of this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole." *Id.* at 764.

¶ 51. That exposure to one person may harm one's privacy interests more than exposure to another person is a familiar feature of human experience. If an embarrassing or humiliating piece of personal information must be revealed to someone, it is surely worse to have it revealed to the neighborhood busybody or to one's boss than it is to have it revealed to a stranger. *See Beaumont v. Brown,* 257 N.W.2d 522, 531 (Mich. 1977) ("Communication of embarrassing facts about an individual to a public not concerned with that individual and with whom the individual is not concerned obviously is not a 'serious interference' with plaintiff's right to privacy, although it might be 'unnecessary' or 'unreasonable.' An invasion of a plaintiff's right to privacy is important if it exposes private facts to a public whose knowledge of those facts would be embarrassing to the plaintiff."), *overruled in part on other grounds by Bradley v. Saranac Cmty. Schs. Bd. of Educ.,* 565 N.W.2d 650, 658 (Mich. 1997). Given that privacy interests are, in this way, deeply sensitive to the identification of the recipient of the information, and given that these interests are what undergird the warrant requirement in the first place, there is no reason that the warrant process should be barred from exhibiting a similar sensitivity.

¶ 52. The reason that we care about who receives the information is because what others know about us shapes our interactions with them. Exposure of embarrassing information to one's neighbor or one's boss is a greater injury because it may impair one's relationships with those people. In contrast,

exposure to a person who will not care or with whom one is unlikely to ever interact causes less harm, even if it may still be a source of reasonable discomfort. This is because one of our central privacy interests is relational – it concerns our ability to foster functional relationships with others. *See* Fried, *supra,* at 480-83 (arguing that privacy is important because it allows us to build relations of trust with others); *see also State v. Geraw,* 173 Vt. 350, 365, 795 A.2d 1219, 1230 (2002) ("Analysis of privacy expectations . . . requires an evaluation of the values intended to be protected by Article 11, such as the exchange of thoughts and ideas, personal trust between individuals, free expression and individuality. . . ."). Our interests in privacy have to do with relating to others on our own terms.

¶ 53. A citizen's relationship with a police officer engaged in an investigation is asymmetric in power and laden with potential consequences. Unlike virtually any other person, an investigating police officer has the power to place a citizen at the mercy of the State. We have the greatest interest in keeping our private information from someone who could do the most damage with it. Moreover, the police officer is necessarily inquisitive. It is the detective's job to be skeptical, probing, and sometimes even relentless. Finally, the police officer assigned to a case is, by definition, not a detached individual and therefore inevitably has a certain perspective.

¶ 54. As a result of all of these features, it is natural to view exposure to a third party – insofar as

exposure is required at all – as less of a setback to one's privacy interests than exposure to an investigating officer. In fact, the protections of the Fourth Amendment are built around the recognition that one's relationship with a detached third party will be different than with an investigating officer. *See Johnson v. United States,* 333 U.S. 10, 13-14 (1948) ("The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.").

¶ 55. The recognition that exposure to a disinterested third party may be substantially less injurious than exposure to an interested party explains why we often rely upon third-party screening in other contexts. For example, third-party filtering or screening teams are frequently used to protect against the disclosure of privileged documents. *See, e.g.*, *Hicks v. Bush,* 452 F. Supp. 2d 88, 103 (D.D.C. 2006) (allowing use of "filter teams" to protect attorney-client privilege with regard to mail seized from Guantanamo Bay detainees); *United States v. Grant,* No. 04 CR 207 BSJ, 2004 WL 1171258 (S.D.N.Y. May 25, 2004) (endorsing government's proposed "privilege team" to screen seized documents for privileged materials); *United States v. Triumph Capital Grp., Inc.,* 211 F.R.D. 31, 43 (D. Conn. 2002) ("The use of a taint

team is a proper, fair and acceptable method of protecting privileged communications when a search involves property of an attorney."); *United States v. Hunter,* 13 F. Supp. 2d 574, 583 (D. Vt. 1998) (accepting the use of "screening procedure designed by the government" in order to "limit invasion of confidential or privileged or irrelevant material").

¶ 56. Courts have also approved of the use of third parties to assist in executing searches where the assistance will help limit the search to the relevant material. *See, e.g.*, *Forro Precision, Inc. v. Int'l Bus. Mach. Corp.,* 673 F.2d 1045, 1054 (9th Cir. 1982) (approving of use of IBM employees in performing a search where "search warrant required that technical documents be identified"); *see also Wilson v. Layne,* 526 U.S. 603, 611 (1999) (approving of "the presence of the third parties" where their presence "directly aid[s] in the execution of the warrant"). The use of third parties can provide an intermediate option between straight disclosure and filtering by a special master or a court in camera. *Cf.*, *e.g., United States v. McClure,* No. 10-028, 2010 WL 3523030, at *2 (E.D. La. Sept. 1, 2010) ("The subpoenaed documents at issue satisfy [the subpoena requirements] but only to the degree that they are probative. . . . To the extent that the requested information does not relate to [the case], the subpoena drifts in the direction of an impermissible 'fishing expedition.' Thus, an *in camera* evaluation would be appropriate to filter out information not probative. . . ."); *Konle v. Page,* 556 N.W.2d 380, 383 (Wis. Ct. App. 1996) ("Because tax returns

will often contain material which is wholly irrelevant to the [case in question], we conclude that an in camera examination by the trial court is the best and proper procedure through which to filter such discovery demands."). In all of these circumstances, it is never assumed that because the information will be revealed to some third party – be it a "filter team," a computer expert, a special master, or a court in camera – the individual concerned retains no residual interests in nondisclosure.

¶ 57. Not surprisingly, courts and commentators have been drawn to these tools for the purposes of mitigating the invasiveness of computer searches. The judicial officer in this case was putting into effect these proposed legal innovations. *See, e.g.*, *CDT II,* 621 F.3d at 1180 (Kozinski, C.J., concurring) (recommending that "[s]egregation and redaction of electronic data must be done either by specialized personnel or an independent third party"); J. Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches,* 79 Fordham L. Rev. 2809, 2857 (2011) (advocating for a requirement that special masters be used "to segregate data that is within the scope of the warrant, while excluding non-relevant evidence unless it closely relates to the crime specified in the warrant or is contained in the same file as evidence that the warrant authorizes to be seized"); Recent Case, *Fourth Amendment – Plain View Doctrine – En Banc Ninth Circuit Holds that the Government Should Waive Reliance on Plain View*

Doctrine in Digital Contexts, 123 Harv. L. Rev. 1003, 1010 (2010) (calling for a procedure in which "[d]esignated computer personnel or a third party would perform a search of the entire hard drive" and "[a]ll responsive information would be culled"). In the computer search context, using a disinterested third party is a natural way to protect a person's interest in who will view personal information.

¶ 58. The interest in who will view personal information is heightened when the information in question is not a single embarrassing fact but rather a vast array of private materials. Personal computers often store every aspect of a citizen's personal life. *See* O. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L. Rev. 531, 533 (2005) ("Computers are like containers in a physical sense, homes in a virtual sense, and vast warehouses in an informational sense."). Without caution, searches of computers threaten to authorize police culling through more personal information than has ever been possible before. *See* R. Winick, *Searches and Seizures of Computers and Computer Data,* 8 Harv. J.L. & Tech. 75, 78 (Fall 1994) ("[T]he massive storage capacity of modern computers creates a high risk of overbroad, wide-ranging searches and seizures.").

¶ 59. Because modern computers contain a plethora of private information, exposing them to wholesale searches presents a special threat of exposing irrelevant but damaging secrets. Judge Kleinfeld of the Ninth Circuit puts the point vividly:

There are just too many secrets on people's computers, most legal, some embarrassing, and some potentially tragic in their implications, for loose liberality in allowing search warrants. Emails and history links may show that someone is ordering medication for a disease being kept secret even from family members. Or they may show that someone's child is being counseled by parents for a serious problem that is none of anyone else's business. Or a married mother of three may be carrying on a steamy email correspondence with an old high school boyfriend. Or an otherwise respectable, middle-aged gentleman may be looking at dirty pictures. Just as a conscientious public official may be hounded out of office because a party guest found a homosexual magazine when she went to the bathroom at his house, people's lives may be ruined because of legal but embarrassing materials found on their computers. And, in all but the largest metropolitan areas, it really does not matter whether any formal charges ensue – if the police or other visitors find the material, it will be all over town and hinted at in the newspaper within a few days. . . . Sex with children is so disgusting to most of us that we may be too liberal in allowing searches when the government investigates child pornography cases. The privacy of people's computers is too important to let it be eroded by sexual disgust.

United States v. Gourde, 440 F.3d 1065, 1077-78 (9th Cir. 2006) (Kleinfeld, J., dissenting). These possibilities do not mean that computers cannot be searched. But given the multiplicity and magnitude of the unanticipated injuries that might be inflicted by allowing exposure of an entire computer hard drive, it is understandable to seek precautions that might mitigate such injuries. And given that exposure of embarrassing information to a detached third party constitutes a lesser injury, we conclude that the use of third-party screeners is not so wholly without basis as to constitute an abuse of the judge's discretion.

¶ 60. The State raises practical objections to these requirements. First, the State argues that ex ante instructions will have no practical effect because the reasonableness of any search will be determined ex post, in response to a motion to suppress, and as a result the instructions "cannot be enforced." The whole point of instructions (2), (3), and (4) is to deny the State access to information outside the justification for the warrant and thus avoid disputes over whether such information can be used in a criminal case or otherwise. As we noted at the outset of this opinion, "It is settled law that the search and seizure of evidence, conducted under a warrant, must conform to the requirements of that warrant." *United States v. Brunette,* 76 F. Supp. 2d 30, 42 (D. Me. 1999). The decision in *Richards v. Wisconsin,* upon which the State relies, stands only for the proposition that suppression might not be required where the noncompliance is based on an unanticipated circumstance,

too urgent in nature for the warrant to be amended. 520 U.S. at 395-96 (accepting police decision not to knock and announce after already having had door slammed in their face by suspect upon seeing uniformed individual).

¶ 61. We agree with the State that ex post review will always remain open, but this does not mean that the ex ante instructions are without legal significance. Indeed, our holding today is that there is no constitutional distinction between instructions on how a search will be conducted and other instructions that, for example, relate to when the search must occur. *See* V.R.Cr.P. 41(c) (warrant shall "command the officer to search within a specified period of time not to exceed 10 days").

¶ 62. Second, the State argues that the requirement to use a non-investigator to conduct the search "without the presence or input of the investigator may result in relevant evidence being missed." In responding to this argument, we note that the State chooses the person(s) conducting the search and can ensure that the person(s) have the skill to recognize relevant evidence. Further, the concept of a firewall does not preclude the State from educating the person(s) conducting the search in the nature alleged crimes, as long as the person(s) conducting the search do not share extraneous information with the State investigator. We do not conclude that there is a practical defect in the condition.

¶ 63. Third, the State argues that the segregation requirement will prevent a dynamic investigation in which the search can be expanded based upon what information is uncovered. Again, we find that the State overstates the objection. Nothing in instruction 5 states that on receipt of information from the search, the criminal investigator cannot ask for additional searching specifying the relevance of additional evidence in light of what evidence was produced.

¶ 64. We therefore deny the request for extraordinary relief with regard to instructions (2), (3), and (4). This result is based largely on the broad authorization sought by the applicant law enforcement officer and the affidavit supporting that application. The judicial officer concluded that resorting to a neutral third-party screener may be the only way to provide meaningful privacy protections in the face of broad law enforcement requests like this one. *See CDT I,* 579 F.3d at 1007 ("In the end . . . we must rely on the good sense and vigilance of our magistrate judges, who are in the front line of preserving the constitutional freedoms of our citizens while assisting the government in its legitimate efforts to prosecute criminal activity. Nothing we could say would substitute for the sound judgment that judicial officers must exercise in striking this delicate balance."). We hold that such an order does protect a legitimate privacy interest and did not constitute a manifest abuse of discretion.

C.

¶ 65. Next, we turn to the instructions limiting the search techniques that police can employ and prohibiting the use of sophisticated searching software without prior court authorization. The judge directed police to use a search protocol "designed to uncover only the information for which the State has probable cause" by focusing on documents limited by: the time period relevant to the alleged criminal activity, key words, and specific file types. The judge also precluded use of sophisticated search techniques without prior authorization.[23]

¶ 66. Under the order, these instructions are imposed on the persons(s) who conduct the search under instruction (2) and were within the court's power to ensure satisfaction of the probable cause and particularity requirements of the Fourth Amendment and Article 11. As noted, the warrant application sought to examine every file on every type of electronic media found at the location listed in the warrant, regardless of ownership. In the judicial officer's view, this application did not provide probable

[23] For example, the judge precluded law enforcement from employing "sophisticated hashing tools." These tools are often used in specialized investigations to identify files containing child pornography. As another court explained: "A hash value and signature analysis of files on a computer hard drive creates a 'fingerprint' of each file on the computer. Once generated, those hash values can be compared to the hash values of files known or suspected to contain child pornography." *State v. Bellar,* 217 P.3d 1094, 1112 n.12 (Or. Ct. App. 2009).

cause for such a broad search without some further specification of the particular places to be searched and the particular items to be seized.

¶ 67. As we have already discussed, especially in a non-physical context, particularity may be achieved through specification of how a search will be conducted. The purpose of the particularity requirement is to prevent general searches. *Maryland v. Garrison,* 480 U.S. 79, 84 (1987). By limiting the authorization to specific areas and specific things, the particularity requirement ensures that the search will be carefully tailored to its justifications and will not become a wide-ranging, exploratory search that the Fourth Amendment prohibits. *See United States v. Carey,* 172 F.3d 1268, 1271-72 (10th Cir. 1999) ("The Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings."). Particularity is measured in practical terms. *United States v. Johnson,* 541 F.2d 1311, 1313 (8th Cir. 1976) (per curiam) (explaining that standard to determine whether warrant describes place to be searched with sufficient accuracy "is one of practical accuracy rather than technical nicety").

¶ 68. The warrant application here asserted the need for a broad, unconstrained search based on the investigating officer's general contention that criminals often hide incriminating evidence by using non-identifying titles, changing file extensions, and encryption or password protection. There was no

information presented, however, that there was reason to believe the suspect in this case had used such techniques or even that those engaged in identity theft typically do so. *Cf. Wolf v. State,* 266 P.3d 1169, 1173-74 (Idaho Ct. App. 2011) (concluding there was sufficient probable cause to search computer hardware, software and electronic devices where affidavit explained officer's experience in area of child exploitation and storage of child pornography on computers).

¶ 69. The application suggests, if not admits, that the broadest scope of search may not be necessary. The affidavit explains that in some cases, the sought-after information can be found through targeted searches not requiring such exhaustive measures. Further, there was no attempt to limit the search based on the known details of the suspected crime such as the time-period, the victim, or the institutions involved in the suspected identity theft. *See Otero,* 563 F.3d at 1132-33 (concluding that warrant application to search computer failed to satisfy particularity required where search was not limited by date and crimes suspected); *United States v. Clough,* 246 F. Supp. 2d 84, 87 (D. Me. 2003) (holding warrant failed to meet particularity requirement where it contained "no restrictions on the search, no references to statutes, and no references to crimes or illegality").

¶ 70. Given that narrowing the search could still accomplish recovery of the incriminating evidence which there was probable cause to believe

would be found within the digital equipment seized, the court was within its discretion to reduce preliminarily the scope of the warrant. The judicial officer did not abuse his power by restricting law enforcement's search to those items that met certain parameters based on dates, types of files, or the author of a document. *See United States v. Rude,* 88 F.3d 1538, 1551 (1996) (concluding that "the specification of dates, individuals, and the [particular] corporation, along with a reasonably precise delineation of the type of records sought, satisfied the specificity requirement").

¶ 71. This was especially appropriate where the State proposed no limiting instructions of its own. The State fails to demonstrate that such limits were overly particular or otherwise untenable. In fact, such limits are essential to meet the particularity requirement of the Fourth Amendment, especially in cases involving record searches where nonresponsive information is intermingled with relevant evidence. *Hunter,* 13 F. Supp. 2d at 582-83 (concluding that particularity requirement was satisfied where records to be seized were identified "by time period and by the individual, entity, or property involved"); *Commonwealth v. McDermott,* 864 N.E.2d 471, 487 (Mass. 2007) (concluding that warrant was sufficiently particular where category limited by time frame and nature of items to be seized).

¶ 72. We recognize that instructions 5 and 6 are less necessary when the search is conducted by persons segregated behind a firewall from State

investigators. Nevertheless, they can be an additional safeguard to guarantee that the search conducted by the segregated persons is not too broad. Indeed, the State in its brief recognized such a need when it observed that "the forensic examiner is as likely or unlikely to conduct an illegal general search of the computer as the investigator." We conclude that their imposition was within the judicial officer's discretion.

¶ 73. Again, the State raises a practical objection that the judicial officer will not have the expertise to review search protocols under instruction (6) and that limitations on search protocols are unworkable because of the dynamic nature of a search. All the instruction calls for is that the persons conducting the search, prior to using hash protocols or similar search tools, educate the judicial officer on the need for these methods and obtain approval. Just as a judicial officer is expected to expeditiously respond to a search warrant request, we can expect timely response to a request to employ special search protocols. We also believe that the judicial officer can be educated on the purpose and method of any search tool, such as to responsibly exercise the oversight responsibility.

¶ 74. Absent grounds to conclude that a judicial officer acted arbitrarily, we will not second-guess the judicial officer's discretionary judgment in the context of a motion for extraordinary relief. *See Richardson v. City of Rutland,* 164 Vt. 422, 424, 671 A.2d 1245, 1247 (1995) (explaining that extraordinary relief in the nature of mandamus is a limited remedy to

correct "an arbitrary abuse of . . . power" (quoting *Couture v. Selectmen of Berkshire,* 121 Vt. 359, 361, 159 A.2d 78, 80 (1960))). The State is not persuasive in its claims that the limits will unduly hamper detection of crime. The equipment is seized and secured in the State's possession. After exhausting its search options as permitted by the conditions of particularity, nothing precludes the State from seeking a new warrant to employ more sophisticated search techniques or a more probing analysis of the electronic media based on the results – or frustration – of their initial search, providing probable cause remains. The State's request for extraordinary relief from these instructions is therefore denied.

D.

¶ 75. Finally, we address those instructions pertaining to the copying, return, and destruction of property. The judicial officer set instructions requiring that: (1) only responsive information could be copied; (2) non-responsive data should be returned and the court informed; (3) copies must be destroyed absent judicial authorization otherwise; and (4) the return should specify the information seized, returned, and destroyed.

¶ 76. These instructions would hardly seem novel if imposed on law enforcement at the initial search phase. It goes without saying that law enforcement officers are empowered to seize and copy only items that are responsive to a warrant and, in

turn, to inventory the items seized and return this list to the court. Indeed, under the Rules of Criminal Procedure, law enforcement officers conducting a search are required to give the person from whom property is taken "a receipt." V.R.Cr.P. 41(d). The officer must also make and file with the court a return, including a written inventory of the property taken. *Id.* The rule allows a grieved individual to move for return of property seized illegally. V.R.Cr.P. 41(e).

¶ 77. In this case, the unique aspect of these instructions arises because the warrant authorized law enforcement to seize electronic medium to be searched off-site. As we noted initially, we are really dealing with two searches here. Apparently, the judicial officer wished to emphasize that although the State was authorized to search off-site, this did not provide authority for the State to retain indefinitely all electronic data and law enforcement was still required to return or destroy nonresponsive data as well as to notify the court of the items retained and returned. Given that the judicial officer's instructions essentially echo the requirements of Rule 41, we conclude that it was within the officer's power to impose them.

¶ 78. In reaching our conclusion, we do not conclude that instruction (7) or (8) prevents the segregated search persons from imaging the computer hard drive and other electronic storage media so that the computer and media can be returned to its owner. That procedure gives the State full search

capacity while minimizing the interference with the activities of the computer owner. It was used in this case.

¶ 79. Instruction (7) prohibits giving copies of extraneous information to State investigation agents. It does not prohibit the persons conducting the search from making copies or images for their own use as long as they are destroyed, as provided in instruction (9).

¶ 80. Nor do we read instruction (9) as prohibiting the maintenance of evidence for appeals, post-conviction relief and civil liability, as the State claims. In circumstances where the State can show that digital information should be kept for a specific reason – for example, for an appeal of a dispute over the validity of or compliance with ex ante instructions – the instruction authorizes the State to seek a judicial authorization to delay destruction. Otherwise, the overall procedure leaves a sufficient record for future proceedings.

¶ 81. Finally, we reject the State's argument that instruction (10) imposes an arbitrary time limit on the search, even though the search may take a long, indeterminate time to finish. Although instruction (10) authorizes the judicial officer to impose a time limit in the warrant on completing the search and filing a return, the warrant itself imposes no time limit and authorizes the analysis be conducted "as long as reasonably necessary." Under these circumstances, the State's argument is premature. In

any event, we reiterate that there are two searches here and just as the applicable criminal rule can impose a time limit on the initial search of the dwelling, *see* V.R.Cr.P. 41(c), the magistrate can impose a time limit on the second.

¶ 82. In sum, we conclude that the judicial officer did not contravene his power in imposing instructions concerning the manner of the law enforcement's search of the computer to satisfy the probable cause and particularity demands of the warrant requirement. However, we hold there was no authority to preclude law enforcement's seizure of items in plain view.

The petition for extraordinary relief is granted in part, and condition (1) is stricken from the warrant. In all other respects, the petition is denied.

FOR THE COURT:

_____

Associate Justice

¶ 83. **BURGESS, J., concurring and dissenting.** Much of what the majority holds today is correct. Nothing in the Fourth Amendment precludes a magistrate from imposing ex ante warrant conditions to further constitutional objectives such as particularity in a warrant and the least intrusion necessary to accomplish the search. *See Andresen v. Maryland,* 427 U.S. 463, 482 n.11 (1976) (recognizing

that, in searches for papers, innocuous documents will be examined to determine if they are subject to the warrant, and admonishing that responsible officials, "including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy"); *see also United States v. Payton,* 573 F.3d 859, 864 (9th Cir. 2009) ("We believe that it is important to preserve the option of imposing conditions when they are deemed warranted by judicial officers authorizing the search of computers."). Nor may a judge simply forbid, ipse dixit, the seizure of criminal evidence found in plain view during a legally authorized search.[24] *See United States v. Stabile,* 633 F.3d 219, 241 (3d Cir. 2011) (holding that plain view doctrine "applies to seizures of evidence during searches of computer files," while acknowledging that the extent of plain view "will vary from case to case").

¶ 84. Thus, I generally concur in denying the State's petition to strike conditions five through ten,

---

[24] "The plain view doctrine is grounded on the proposition that once police are lawfully in a position to observe an item first-hand, its owner's privacy interest in that item is lost; the owner may retain the incidents of title and possession but not privacy." *Illinois v. Andreas,* 463 U.S. 765, 771 (1983). Therefore, an object lawfully viewed, the incriminating character of which is immediately apparent, may be seized without any resulting privacy invasion. With no constitutionally protected privacy interest threatened, there is no Fourth Amendment authority to prevent law enforcement from seizing items of a criminal nature in plain view.

which focus the search while not defeating the law,[25] and concur in granting the State's petition to strike the first condition purporting to cancel the plain view doctrine. But, having just reiterated the long-settled rule that police can seize evidence of a crime observed in plain view during a valid search, the majority errs in turning about-face to uphold conditions that the search be conducted by police agents separated from the case investigators, and who are not to look at, tell about, or must pretend not to see, any plainly visible evidence of other crimes. These limits are contained in warrant conditions (2), (3), and (4) and are expressly designed to frustrate the plain view doctrine. Because this latter holding is not rooted in any constitutional principle or privacy protection, I respectfully dissent.

¶ 85. Casting this dissent as promoting a law enforcement "right" to plain view in derogation of defendants' rights, *ante,* ¶ 45, the majority correctly suggests a competition between law enforcement and privacy rights. But, the competition is settled. We have a right against unreasonable search and seizure under the Fourth Amendment. It is black-letter law that, under the same Amendment, police are authorized or, to use the majority's term, have a "right" to

[25] Condition (7), however, which directs that only evidence related to the targeted activities may be copied, should be modified to allow copying and retention of any other contraband or incriminating evidence constitutionally observed in plain view.

search pursuant to a valid warrant. Since our privacy is already compromised by such a warrant, it is equally beyond cavil that in executing the valid search for specified evidence, another object lawfully viewed, the incriminating character of which is immediately apparent, may be seized without any resulting privacy invasion. *Minnesota v. Dickerson,* 508 U.S. 366, 374-75 (1993); *see also Horton v. California,* 496 U.S. 128, 1333-34 (1990) ("If an article is in plain view, neither its observation nor its seizure would involve any invasion of privacy."). Whatever limitation the majority invents to prohibit seizure of incriminating evidence in lawful plain view, it is outside of the Fourth Amendment.

¶ 86. The majority's closest facsimile to authority are the shunted, if not politely discredited, conditions from *United States v. Comprehensive Drug Testing, Inc. (CDT I),* 579 F.3d 989 (9th Cir. 2009) (en banc), that the government waive plain view and segregate its searchers as predicates to obtaining warrants to search computers. Responding to egregious overreaching by federal agents executing a warrant for computer records of steroid use in major league baseball, *CDT I* directed magistrates to deny or curtail computer search warrants unless the government agreed to "forswear" the plain view doctrine and employ segregated screener-searchers held incommunicado from the primary investigators. *Id.* at 998. It was *CDT I* that apparently inspired the issuing court here to interdict plain view.

¶ 87. Since the trial court's reliance on *CDT I,* however, those conditions limiting plain view were effectively reversed by the entire Ninth Circuit specially convened to review the issue. *United States v. Comprehensive Drug Testing, Inc. (CDT II),* 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam). The original ex ante directives limiting plain view and imposing segregated searcher-screeners were deleted by the full court, and relegated to a mere recommendation marooned in a concurring opinion. *CDT II,* 621 F.3d at 1180 (Kozinski, C.J., concurring). Even that concurrence concedes that its recommendations are "guidance" only and not mandated. *Id.* at 1178; *see United States v. Ganias,* No. 3:08CR00224(AWT), 2011 WL 2532396, at *6 (D. Conn. June 24, 2011) (denying motion to suppress and pointing out that *CDT II* may provide guidance, "but it does not provide a rule that must be complied with").

¶ 88. Despite claiming that courts are "drawn to" such tools to mitigate invasiveness of computer searches, *ante,* ¶ 57, the majority cannot find a court that adopts Chief Justice Kozinski's concurring "guidance" in CDT II. Courts do, however, consistently reject it. *See Stabile,* 633 F.3d at 240-41, 240 n.16 (upholding plain view seizure during search of computer files, reserving review on case-by-case basis and expressly "declin[ing] to follow the Ninth Circuit's suggestion to 'forswear reliance on the plain view doctrine'" as proposed in the *CDT II* concurrence (quoting *CDT II,* 621 F.3d at 1178 (Kozinski, C.J., concurring))); *United States v. Mann,* 592 F.3d 779,

785 (7th Cir. 2010) (upholding plain view seizure during computer search, and refusing to "jettison[ ]" plain view or apply the original *CDT I* search conditions, observing that "there is nothing in the Supreme Court's case law (or in the Ninth Circuit's for that matter) counseling the complete abandonment of the plain view doctrine in digital evidence cases"); *Ganias,* 2011 WL 2532396, at *6; *United States v. Farlow,* No. CR-09-38-B-W, 2009 WL 4728690, at *6 & n.3 (D. Me. Dec. 3, 2009) (denying motion to suppress, characterizing C.J. Kozinski's preclusion of plain view as "unwise," and observing that "no other [court] has gone so far as the Ninth [Circuit] to require such significant preconditions on the issuance of search warrants for computers"). Unable to arrive at any Fourth Amendment basis or need for the conditions in this case, this Court should likewise reject such extra-constitutional recommendations and adhere to the plain view doctrine approved under the Fourth Amendment.

¶ 89. It bears noting that the majority holding is not, like the suppression of illegally obtained evidence, fashioned to vindicate a constitutional right. The underlying search warrant is entirely lawful without the majority's gag condition and segregated searchers, and presents no violation of any privacy right guaranteed against unreasonable search and seizure. No one complains that the warrant is insufficiently particular. The majority agrees there is no constitutional limitation on observing evidence of other crimes in plain view during a valid

search. The majority can point to no infraction of the Fourth Amendment, actual or threatened, to justify its ex ante limits on plain view. Given that the warrant application is otherwise valid, the majority's holding provides little instruction to the trial bench on when and how to apply such segregated searches in the future since no constitutional right requires application of this extraordinary measure.

¶ 90. Further, whatever computer privacy the majority supposes to protect will be already and completely compromised by the warrant and the search, even when executed by the majority's gagged search team. Whether viewed by the case investigator or segregated police, or some other police agent, the court-ordered privacy invasion is the same.[26] These conditions mean that just as much private information will be exposed to the view of government strangers. As acknowledged and argued by amicus ACLU, "the harm to privacy interests is complete when the protected material is viewed." In real life, requiring that a search be executed by one police agent versus another results in no actual limit on the search and, so, no actual protection of privacy.

¶ 91. The majority's segregated screening conditions result in no less of a search, no less intrusion

[26] Even if the State secured a private entity to execute the warrant, as contemplated by the issuing court, it would be no less a governmental search. *See United States v. Richardson,* 607 F.3d 357, 364 (4th Cir. 2010).

into the computer's files, and no less potential for observing other incriminating evidence in plain view of the searchers. Thus, requiring a search by different, segregated and muted investigators serves no Fourth Amendment privacy interest whatsoever. Protecting no actual privacy, the majority simply conjures up immunity for computer owners whose data includes proof of other crimes in plain view during a valid search. At the same time, such immunity does not exist for property holders whose homes, bedrooms, closets, file cabinets, files, and purses are lawfully searched – because the constitution does not require it.

¶ 92. Nor does the constitution require such immunity for computer content. If the issuing court was concerned about lack of probable cause or particularity as the majority asserts, *ante,* ¶ 43, then the court was free to deny the warrant application or limit the search accordingly. Neither probable cause nor the application's particularity is challenged here. The majority's endorsement of the silenced-and-segregated-search-team condition succeeds in defeating actual plain view, but utterly fails to increase particularity or narrow the scope of the search. As noted above, the search – the actual invasion of privacy applied for by the State and authorized by the warrant – is exactly the same, whether conducted by investigators assigned to the case, or by the judicially gagged investigators preferred by the majority.

¶ 93. Patently incorrect is the majority's assertion that investigators will never view incriminating

evidence unrelated to identity theft offenses. The majority imagines that ordering the search be conducted by police investigators not assigned to *this* investigation somehow "obviate[s]," or prevents, plain view from occurring. *Ante,* ¶ 37. If this were true, there would be no need for the gag order. But since it is clear that plain view of other incriminating evidence by the other police search team can still occur, the supposed prevention can only result from the gag order that prevents its disclosure. Thus, declares the majority, gagging the search team is "not an abrogation of the plain view doctrine," but a safeguard "against the police plainly viewing." *Ante,* ¶ 44. All winking aside, the search is still authorized by the warrant, privacy is still invaded by government search agents, and any other evidence in plain view is still seen. The old saying about being "just a little bit pregnant" comes to mind. That adage, of course – like pretending a search is not a search, and that evidence in plain view is not seen or even does not exist – is a fallacy.

¶ 94. There is not cited a single Fourth Amendment case to support the majority's sabotage of the plain view doctrine. This is because the Fourth Amendment expressly proscribes unreasonable searches, and it is undisputed that a search authorized by a warrant supported by probable cause and approved by a magistrate is not unreasonable. It is equally settled that where a magistrate authorizes a valid search under the Fourth Amendment, there is no constitutionally protected privacy against such an

intrusion. Certainly most people prefer that police not enter their homes or computers to search, but if a warrant issues then the proprietor is without right to resist. *See Gasho v. United States,* 39 F.3d 1420, 1432 n.12 (9th Cir. 1994) (recognizing that "a citizen has no right to resist a search or seizure pursuant to a warrant").

¶ 95. The majority's notion, to limit judicial warrants according to what boils down to an aversion to police viewing or disclosing evidence of what could be our criminal misconduct – in other words, to have criminals set the standard – is patently unworkable and is not the law. Once a warrant validly issues, it is irrelevant whether the target likes the police, wants to disclose information to the police, or would choose someone else to conduct the search. It has never been held otherwise.

¶ 96. Finding no support in the law of search and seizure, the majority seeks a rationale from rulings in civil litigation over unauthorized exposures of private information. The majority's distinctions between different disclosures and degrees of embarrassment make for an interesting exploration of the multi-faceted nature of privacy and our varied reactions to having secrets revealed to some people as opposed to others, *ante,* ¶¶ 50-53, but the Fourth Amendment is all about *searches* and not about disclosure. Truisms about the need to protect citizens from state intrusion are exactly why the constitution limits the government's authority to search us and our belongings.

¶ 97. The Fourth Amendment's protection against unreasonable search and seizure does not turn on some sliding scale of privacy or potential embarrassment. All of our private spaces, regardless of perceived or relative importance, are protected to the same degree: the government may not obtain a search warrant except upon probable cause and with particularity. *See New Jersey v. T.L.O.,* 469 U.S. 325, 335-39 (1985) (explaining that the Fourth Amendment does not compare privacies, but protects against "arbitrary invasions by government officials," be they police or civilian authorities, whether searching children, adults or any of their closed containers). Which police agent conducts the search is generally irrelevant to whether the search is reasonable. *Id.* at 335 (applying the constitutional strictures not only to police searches, but to inspections by any "sovereign authority").[27] The constitutional point is not who gets

[27] To be sure, as noted by the majority, police may, in special circumstances not posed here, propose or accede to assistance of specialists to execute a search warrant. *See United States v. Schwimmer,* 692 F. Supp. 119, 126-27 (E.D.N.Y. 1988) (denying motion to suppress when a private computer expert assisted in search and such assistance was permitted by warrant). Searching a law office may require a special search team to separate documents and preserve attorney-client privilege. *See In re Impounded Case (Law Firm),* 840 F.2d 196, 199 (3d Cir. 1988); *United States v. Hunter,* 13 F. Supp. 2d 574, 583 (D. Vt. 1998) (affirming use of screening procedure to separate privilege-protected documents and endorsing use of special master). There is no analogous circumstance in the instant case to justify extra-screening measures. No privilege is implicated. No special

(Continued on following page)

to share evidence discovered in a legal search, but whether the government can search at all.

¶ 98. In this case, the constitutional question was answered when the magistrate issued the warrant on what the parties do not dispute was probable cause. Appropriate restrictions on the search itself were imposed by the issuing court to ensure particularity and to avoid an unfettered search as commanded by the Fourth Amendment. Ex ante conditions (5) and (6) limited police to methods likely to find only the evidence specifically sought, and prohibited escalation of the search with more sophisticated tools without prior judicial approval. In contrast, the conditions imposing a segregated, silenced or blinkered search team and no sharing of evidence in plain view adds no particularity, limits no search, serves no privacy and the majority cannot show us where it is called for by the constitution.[28]

---

discriminatory skill not possessed by law enforcement is required to search for what the warrant here authorizes.

[28] In any event, Fourth Amendment safeguards on plain view are already in place. To avoid suppression, police must demonstrate that any item seized, but not covered by the warrant, was (1) discovered from a lawful vantage point, *Kentucky v. King,* ___ U.S. ___, ___, 131 S. Ct. 1849, 1858 (2011), and (2) the criminal nature of the item was immediately apparent – that is, there must be contemporaneous probable cause to believe the object plainly seen is contraband, stolen property or evidence of a crime. *Arizona v. Hicks,* 480 U.S. 321, 326-27 (1987). In the context of voluminous documents, not dissimilar to computer files here, plain view is not open to any on-the-scene quest for supporting probable cause, since the text of documents

(Continued on following page)

¶ 99. Assuming that searching a computer can challenge traditional notions of privacy,[29] the challenge is missing in this case. What the State seeks to look for, and where, seems hardly different from a search for files in a cabinet, papers in a desk, drafts in a checking account or letters in a box. To the extent that depth or volume of data is the issue, if the necessary probable cause is made out, a warrant can issue to find a needle in a haystack or a needle in a house or office.

¶ 100. Moreover, given no dispute that the State may seize incriminating evidence noticed in plain view during an otherwise valid search, those restrictions are a bald interference by the judiciary in the legal execution of a warrant by the executive branch. The majority can refer to no case or rule authorizing the court to command blindness or feigned ignorance to a constitutionally authorized plain view of criminal evidence. Eliminating plain view ad hoc in a particular search through the ex

---

may be viewed only to the extent necessary to initially determine if the documents may be seized under the warrant. *Andresen,* 427 U.S. at 482 n.11; *see United States v. Rude,* 88 F.3d 1538, 1552 (9th Cir. 1996) (delineating that officers conducting a search are permitted to peruse documents to determine if they fall within scope of warrant, but may not minutely scrutinize their contents).

[29] It has been opined, however, 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. Upham,* 168 F.3d 532, 535 (1st Cir. 1999).

ante artifice of a separate and gagged search team achieves exactly what the majority acknowledges is improper, *ante,* ¶ 38: leaving the magistrate "to disregard the considered limitations of the law" (like the court's lack of authority to proscribe plain view), and conferring "on a judicial officer the authority to pick and choose what legal doctrines would apply to a particular police search" (as in commanding police to ignore evidence in plain view in a computer search, while allowing plain view discovery in a house or office search).

¶ 101. The separation and screening condoned by the majority does not protect actual privilege or privacy, does not further a Fourth Amendment privacy interest, and does not lend further particularity to the search. The sole purpose of the segregation and gag order is to discard the plain view doctrine – something the majority already agrees is beyond the issuing court's authority. I must dissent, and am authorized to state that Chief Justice Reiber joins this concurrence and dissent.

Associate Justice

STATE OF VERMONT

SUPERIOR COURT CRIMINAL DIVISION
Chittenden Unit

In re: Application for Search Warrant
Eric Gulfield Computer

AMENDED ORDER

The application to search the computer belonging to Eric Gulfield is *granted* subject to the conditions listed herein. In setting these conditions, the Court has been guided by *United States v. Comprehensive Drug Testing, Inc.,* 579 F.3d 989 9th Cir. 2009) [sic].

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 ~~threats~~ [offenses s/ MSK] being investigated must be segregated and redacted before it is provided to the State, no matter how intermingled it is.

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.

Dated at Burlington, Vt., December 22, 2010

/s/ Michael S. Kupersmith
Michael S. Kupersmith
Superior Judge

ORIGINAL

STATE OF VERMONT
CHITTENDEN COUNTY, ss.

SEARCH WARRANT

TO: Det. Michael D. Warren and any Vermont Law Enforcement Officer:

You are hereby commanded to search:

- [Address Omitted] Burlington, Vermont. [Address Omitted] is described as a one level single family residence with crème color siding, red shutters, a red garage door and the number [Address Omitted] displayed to the right of the front main door. [Address Omitted] is located by taking the second, most westerly entrance to [Address Omitted] and traveling all the way to the end. The house is the last house on the east side of the street prior to the street looping around back to Starr Farm Road (see pic below)

  [Picture Omitted In Printing]

For the following described property or objects:

- SEE ATTACHMENT "A"

  [See also attached order]

Serving this warrant and making the search of the PREMISES between the hours of ***6AM and 10PM*** within ***ten (10)*** days from the date hereof, and if the property or object be found there, to seize it, prepare a written inventory of it, and bring such property or

object before the District Court of Vermont, Unit No. III.

Continuing, under the authority of this warrant, to conduct a search/analysis of the items seized for the evidence described, for as long as reasonably necessary at an off-site facility or facilities determined by law enforcement.

This warrant is issued upon the basis of an affidavit and the finding of probable cause by me, filed with the clerk of the court.

Dated at Burlington, County of Chittenden, on the 22nd day of December 2010

/s/ Michael S. Kupersmith
Judge @ 1:50 pm.

STATE OF VERMONT
CHITTENDEN COUNTY, ss.

APPLICATION FOR SEARCH WARRANT WITH AFFIDAVIT

A. Application

Det. Michael D. Warren requests the Honorable ***COURT*** to issue a warrant to search:

- [Address Omitted] Burlington, Vermont. [Address Omitted] is described as a one level single family residence with crème color siding, red shutters, a red garage door and the number [Address Omitted] displayed to the right of the front main door. [Address Omitted] is located by taking the second, most westerly entrance to [Address Omitted] and traveling all the way to the end. The house is the last house on the east side of the street prior to the street looping around back to Starr Farm Road (see pic below)

[Picture Omitted In Printing]

For the following described property or objects:

- SEE ATTACHMENT "A"

And if such property or object be found there to seize it, prepare a written inventory of it, and bring it before the District Court of Vermont, Unit No. III.

The applicant has probable cause to believe that such property or object will be found in such premises and on such person and will constitute:

Evidence of the crime(s) of:

- Identity Theft – Title 13 VSA 2030

For the purposes of establishing probable cause for the issuance of this warrant, there are attached hereto the following affidavit:

Affidavit of Det. Michael D. Warren

This application is executed by Det. Michael D. Warren on this 22nd day of December 2010

/s/ Michael D. Warren #193
Det. Michael D. Warren

STATE OF VERMONT
CHITTENDEN COUNTY, ss.

I, Det. Michael D. Warren, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND OFFICER BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Vermont Rules of Criminal Procedure for a warrant to search the premises known as "*[Address Omitted] Burlington, Vermont"* hereinafter "PREMISES," for certain things particularly described in Attachment A.

2. I am a detective with the Burlington Police Department, where I have been since 1998. During my tenure at the Burlington Police Department I have the following experience and training in regards to digital evidence, computers and/or Internet related investigations: I have attended the one week long Internet Crimes Against Children (ICAC) "Investigative Techniques" training in Dallas, TX (October 2009), The Secret Service 36 hour course "Basic Investigation of Computers and Electronic Crimes Program" in Hoover Alabama (March 2010), TLO 28 hour Undercover Internet Peer to Peer Investigation training in Burlington, VT (February 2010), VT ICAC Introduction to computer and internet training in Burlington, VT (October 2008), National White Collar Crime Center "identity theft investigations" at the VPA Pittsford, VT (August 2008). I am

currently assigned to the VT Internet Crimes Against Children Task Force (ICAC) focusing 100% of my time to child sexual exploitation cases. I have also investigated and assisted with multiple cases involving computer facilitated exploitation of children.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Title 13 Vermont Statutes Annotated 2030 makes it a state criminal offense to obtain, produce, possess, use, sell, give, or transfer personal identifying information belonging or pertaining to another person with intent to use the information to commit a misdemeanor or a felony.

THE CURRENT INVESTIGATION

A. On 12-01-2010 I was assigned to investigate an Identity Theft case that had been transferred by the NY State Police. Sgt. Frisbie had taken the initial report from the NYSP investigator who had forwarded copies of his reports and investigation. Sgt. Frisbie then requested that the case be transferred directly to the detective bureau for investigation based on the complexity of the case and the amount of follow-up required.

B. On 12-2-2010 I contacted the victim in the case, J.K. [Name Omitted] DOB: [Date Of Birth Omitted]. I explained to K. that I had

been assigned the case and that I was going to be following up shortly with the case. I provided contact information to K. in the event that he needed to contact me regarding the case. I spoke with K. briefly about the facts of the case. The following is a brief synopsis of the interview with K.

C. K. stated that he had just returned home from a lengthy stay at the hospital where he was being treated for a potentially fatal round of pneumonia. K. said that he is 84 years old and has had a variety of health issues lately and he is frustrated that he also has to deal with someone who is trying to steal his identity. K. advised that he had received a fraud notification alert from a credit report monitoring service regarding his credit file. K. said that he then learned that someone was trying to obtain multiple credit cards. K. stated that he also learned that someone had tried to file an official address change form with the United States Post Office changing his mailing address from [Address Omitted], Lyon Mountain NY to a new address of [Address Omitted] in Burlington, VT. K. stated that he did not request an address change with the USPS and whoever did was doing so without his permission. K. stated that attempts were made to obtain Citi Cards and Kohl's/Chase as well as another that he could not remember the name that called him at home to verify the validity of the account opening.

D. Following my conversation with K. I contacted B.P. [Name Omitted], a senior fraud analyst with the First National Bank of Omaha, regarding the incident. P. provided me with additional paperwork identifying the IP address that was used to attempt to fraudulently obtain a Visa Card. The date and time that the transaction was completed via the internet was 07-16-2010 at 08:56 utilizing an IP address of 24.91.163.40. The credit card application was filled out via the website Visa.com. The application was completed with the following information.

Applicant name:	J.K.
SSN:	(Mr. K.'s true social security #)
DOB:	[Date Of Birth Omitted]
Mother's Maiden Name:	[Omitted]
Address:	[Address Omitted] Burlington, VT 05408
Home Phone #:	(802) [Omitted]
Business Phone #:	(802) [Omitted]
Current Employer:	Hudson Valley
Salary:	$6,083.33/month
Years at address:	29 years
Monthly mortgage payment:	$0
IP Address #:	24.91.163.40
Email Address:	gulfields@aol.com

E. A check of the Burlington Police records indicate that [Address Omitted] is occupied by Eric Gulfield Sr DOB: [Date Of Birth Omitted] with a phone number of 802 [Omitted]. A check of the VT DMV records indicate that Eric Gulfield lists his address as [Address

Omitted] in Burlington. As noted above on the Credit Card application the phone number associated with [Address Omitted] is the same number that is listed in BPD and DMV records for Eric Gulfield. Based on this information I believe that [Address Omitted] is occupied by Eric Gulfield.

F. I next spoke with NYSP Inv. Jerome Miner who assisted with the investigation that occurred in NY. Inv. Miner had subpoenaed Comcast requesting the subscriber for the IP address 24.91.163.40 on 07-16-2010 at 8:56am (the date and time the IP was used to attempt to set up the fraudulent Credit Card). On 09-10-2010 Inv. Miner received records from Comcast indicating that the subscriber of the above listed IP address was B.S. [Name Omitted] of [Address Omitted] Inv. Miner provided me with a copy of the results of the subpoena. Upon learning of the subpoena results I drove by the area of [Address Omitted] and learned that [Address Omitted] is located diagonally across the street within approximately 100 feet. I used a handheld wireless internet (wifi) detector and was able to observe multiple wifi connections within the area. There was only one wifi internet connection that was "open" meaning that it was unsecure and anyone could log on and use the connection to access the internet. It appeared that the signal was strong enough to access from [Address Omitted].

G. On 12-06-2010 I contacted B.S. by phone and explained that I was conducting an investigation relating to computer use and the internet. I asked Ms. S. if I could meet with her to discuss the case. Det. Paul Petralia and I met with S. at her residence at [Address Omitted] at approximately 1830 hrs. The following is a synopsis of the interview with S.

H. S. stated that she currently lives alone and works as a Spanish teacher at Spaulding High School. S. said that he [sic] three kids have all moved out and are attending college in CA, WY, and UT. S. said that her kids have not been home since the beginning of the school year. S. said that she currently only has one computer which is located in the kitchen area. S. said that she primarily uses her computer at work but sometimes accesses the internet from home. S. said that she was aware that her internet connection was open and thought that it was not a "big deal". I explained that she is opening herself up to fraud by using her home computer on an open unsecured system. I explained that I was conducting an investigation in which someone using her internet was applying for fraudulent credit cards in the name of J.K. from upstate NY. S. said that she did not know anyone from upstate NY nor did she know K. S. said that she was in no way involved in any fraudulent applications for credit cards. I asked S. if she would allow me to connect to her wireless router to view the "router log" in an attempt to identify possible

people that were connecting to her wireless internet. I connected my laptop computer to the D-link wireless router and was able to view the Router log. Photos of the 20 pages of logs were taken by me and later attached to the case file. I later reviewed the logs and learned that on multiple occasions during the month of November the router was accessed by a computer with an assigned name of GulfieldProp-PC. It shall also be noted that the email address on the First National Bank of Omaha Credit Card application is *gulfields@aol.com*. I believe that someone utilizing a computer from the Gulfield residence located at [Address Omitted] is using the open wireless connection of B.S. to access the internet.

I. Based upon the above facts I feel that probable cause exists to believe the residence located at [Address Omitted] in Burlington contains evidence of the crime of Identity Theft. I am requesting that the court issue a warrant to search the above listed address for the items detailed in "Attachement [sic] A".

TECHNICAL TERMS

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

   a. **IP Address**: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address typically

looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changing – IP addresses.

b. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

COMPUTERS AND ELECTRONIC STORAGE

6. As described above and in Attachment A, this application seeks permission to search and seize records that might be found on the PREMISES, in whatever form they are found. I submit that if a computer or electronic medium is found on the premises, there is probable cause to believe those records will be stored in that computer or

electronic medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or "slack space" *(space on the hard drive that is not currently being used by an active file)* for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Similarly, files that have been viewed via the internet are typically automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard

drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

7. In this case, the warrant application requests permission to search and seize any and all computers. This affidavit also requests permission to seize the computer hardware and electronic media that may contain evidence and if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. In this case, computer hardware that was used to access the internet and fraudulently apply for credit cars [sic] is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.

8. Because more than one person resides at the PREMISES, it is possible that the PREMISES will contain 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 and stored thereon, this application seeks permission to search and to seize those computers as well.

9. Based upon my knowledge, training and experience, I know that searching for information stored in computers often requires agents to seize most or all electronic storage devices to be searched later by a qualified

computer expert in a laboratory or other controlled environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine those storage devices in a laboratory setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the laboratory setting. This is true because of the following:

a. ***The volume of evidence.*** Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

b. ***Technical requirements.*** Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer

experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis.

10. Searching computer systems for the evidence described in Attachment A may require a range of data analysis techniques. 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. In light of these difficulties, the VT ICAC TF intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

11. *In light of these concerns, I hereby request the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence. In addition, I hereby request the Court's permission to take as long as necessary to conduct the off-site search/analysis of the hardware for the evidence described.*

CONCLUSION

12. Based upon the information in this affidavit, I have reason to believe that, records, evidence, fruits and instrumentalities relating to violations of Title 13 Vermont Statutes Annotated 2030 exists. I submit that this affidavit supports probable cause for a warrant

to search the PREMISES and seize the items described in Attachment A.

(Affiant) Michael D. Warren #193

Subscribed and sworn to before me on the 22nd **day of** December 2010**, in Burlington, Vermont.**

/s/ Michael S. Kupersmith
Judge

ATTACHMENT "A"
DESCRIPTION OF PROPERTY TO BE SEIZED

1. All records relating to violations of the statute listed on the warrant, including:

    a. Any paperwork, mail, credit cards, credit card applications in the name of J.K.

    b. Any correspondence, letters, envelopes, electronic mail, chat logs, electronic documents, diaries, notebooks, notes, address books, mailing lists, address labels, or other documents pertaining to:

        1. Dominion and control over any of the property searched, including but not limited to utility bills, credit card bills, Internet service bills, telephone bills, and correspondence.

2. Any computers or electronic media, including hard disks, magnetic tapes, compact disks ("CD"), digital video disks ("DVD"), cell phones or mobile devices and removable storage devices such as thumb drives, flash drives, secure digital ("SD") cards or similar devices, floppy disks and zip disks (hereinafter "MEDIA") that were or may have been used as a means to commit the offenses described on the warrant.

3. For any computer hard drive or MEDIA that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. Evidence of user attribution showing who used or owned the MEDIA at the time the things described in this warrant were created,

edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history;

b. Passwords, encryption keys, and other access devices that may be necessary to access the MEDIA;

c. Documentation and manuals that may be necessary to access the MEDIA or to conduct a forensic examination of the MEDIA.

Date: 12/22/10 **Signed:** Michael D. Warren #193
Applicant

RETURN OF SERVICE

On December 22, 2010 I executed this Search Warrant and initiated the search on [Address Omitted] in Burlington. Pursuant to the search a Sony Vaio computer model number PCG-7113L (SN 00146-524-056-422) was seized in accordance with attachment "A" of the warrant application. This Computer hard drive was "imaged" by the VT ICAC forensic computer lab however a search of the computers hard drive has not yet been conducted. The search of the computers hard drive will not be conducted until a ruling by the VT Supreme Court is made regarding an attachment to the search warrant that was added as a condition by Judge Kupersmith.

/s/ Michael D. Warren #193 4/7/2011
Detective Michael D. Warren