

IN THE SUPREME COURT OF THE STATE OF VERMONT

IN RE APPEAL OF APPLICATION FOR SEARCH WARRANT

Supreme Court Docket No. 2010-479

On Petition for Extraordinary Relief
From the Superior Court of Vermont, Chittenden Criminal Division

**BRIEF OF THE OFFICE OF THE DEFENDER GENERAL
AS AMICUS CURIAE**

On the brief:

Matthew Valerio, Esq.
Defender General

Rebecca Turner, Esq.
Appellate Defender

Marshall Pahl, Esq.

Office of the Defender General
6 Baldwin St., 4th Floor
Montpelier, VT 05633-3301
(802) 828-3168

STATEMENT OF THE ISSUES

I. THE WARRANT-ISSUING JUDGE HAS AUTHORITY TO IMPOSE ANY REASONABLY APPROPRIATE CONDITIONS TO ENSURE THAT THE WARRANT IS IN FULL COMPLIANCE WITH ARTICLE 11 OF THE VERMONT CONSTITUTION AND THE RULES OF CRIMINAL PROCEDURE13

II. THE STATE’S CLAIM THAT JUDICIAL REVIEW AT THE SUPPRESSION HEARING AND AN OVERALL STANDARD OF REASONABLENESS IS SUFFICIENT PROTECTION OF PRIVACY RIGHTS CONTRAVENES VERMONT LAW18

III. THE COURT’S CONDITIONS WERE WELL WITHIN ITS DISCRETION TO IMPOSE IN ORDER TO SATISFY PARTICULARITY REQUIREMENTS UNDER VERMONT LAW AND TO AVOID A GENERAL WARRANT21

IV. THE COURT’S CONDITIONS WERE WELL WITHIN ITS DISCRETION TO IMPOSE TO ENSURE THAT THERE WAS PROBABLE CAUSE TO SUPPORT THE SEARCH OF THE COMPUTER.....28

V. THE COURT WAS CORRECT AS A MATTER OF LAW THAT THE PLAIN VIEW DOCTRINE DOES NOT APPLY HERE AS THE NECESSARY CONDITIONS ARE NOT TRIGGERED AND IT WOULD HAVE TRANSFORMED THE WARRANT INTO A GENERAL AND OVERBROAD SEARCH31

VI. THE STATE’S FACTUAL CLAIMS OF ADMINISTRATIVE INEFFICIENCIES HAVE NOT BEEN PREVIOUSLY FOUND BY THE JUDGE AND CANNOT BE RESOLVED BY THIS COURT, NOR DO THEY DIMINISH THE PROTECTIONS PROVIDED UNDER ARTICLE 11 AND V.R.CR.P. 4134

TABLE OF CONTENTS

STATEMENT OF THE ISSUES2

TABLE OF AUTHORITIES.....5

STATEMENT OF THE FACTS7

STANDARD OF REVIEW.....10

ARGUMENT11

I. THE WARRANT-ISSUING JUDGE HAS AUTHORITY TO IMPOSE ANY REASONABLY APPROPRIATE CONDITIONS TO ENSURE THAT THE WARRANT IS IN FULL COMPLIANCE WITH ARTICLE 11 OF THE VERMONT CONSTITUTION AND THE RULES OF CRIMINAL PROCEDURE.....13

A. ARTICLE 11 JURISPRUDENCE REQUIRES MORE EXACTING JUDICIAL OVERSIGHT THAN DOES THE FOURTH AMENDMENT..... 13

B. VERMONT’S “LEAST INTRUSIVE MEANS” REQUIREMENT..... 14

C. VERMONT COURTS HAVE RECOGNIZED AUTHORITY TO REGULATE THE MANNER IN WHICH A SEARCH MAY BE CONDUCTED..... 15

II. THE STATE’S CLAIM THAT JUDICIAL REVIEW AT THE SUPPRESSION HEARING AND AN OVERALL STANDARD OF REASONABLENESS IS SUFFICIENT PROTECTION OF PRIVACY RIGHTS CONTRAVENES VERMONT LAW.....18

A. POST-HOC JUDICIAL REVIEW, BY MOTION TO SUPPRESS, OFFERS NO PROTECTION FOR COMPUTER-USERS WHO HAVE NOT BEEN SUSPECTED OF OR CHARGED WITH ANY CRIME 18

B. THE STATE’S POST-HOC “REASONABLENESS” STANDARD PROVIDES NO REALISTIC REMEDY TO PERSONS CHARGED WITH CRIME..... 19

III. THE COURT’S CONDITIONS WERE WELL WITHIN ITS DISCRETION TO IMPOSE IN ORDER TO SATISFY PARTICULARITY REQUIREMENTS UNDER VERMONT LAW AND TO AVOID A GENERAL WARRANT21

A. ARTICLE 11 REQUIRES THAT PARTICULARITY BE SUFFICIENTLY DETAILED TO AVOID A GENERAL WARRANT AND UNCHECKED DISCRETION BY THE GOVERNMENT.....21

B. V.R.CR.P. 41 SETS A HIGH STANDARD FOR PARTICULARITY IN THE WARRANT23

C. A WHOLESALE SEARCH OF ALL ELECTRONIC DEVICES IS THE FUNCTIONAL EQUIVALENT OF A GENERAL WARRANT AND CAPTURES PROTECTED COMMUNICATIONS UNDER THE FIRST AMENDMENT 23

IV. THE COURT’S CONDITIONS WERE WELL WITHIN ITS DISCRETION TO IMPOSE TO ENSURE THAT THERE WAS PROBABLE CAUSE TO SUPPORT THE SEARCH OF THE COMPUTER.....28

V. THE COURT WAS CORRECT AS A MATTER OF LAW THAT THE PLAIN VIEW DOCTRINE DOES NOT APPLY HERE AS THE NECESSARY CONDITIONS ARE NOT TRIGGERED AND IT WOULD HAVE TRANSFORMED THE WARRANT INTO A GENERAL AND OVERBROAD SEARCH.....31

**VI. THE STATE'S FACTUAL CLAIMS OF ADMINISTRATIVE
INEFFICIENCIES HAVE NOT BEEN PREVIOUSLY FOUND BY THE
JUDGE AND CANNOT BE RESOLVED BY THIS COURT, NOR DO THEY
DIMINISH THE PROTECTIONS PROVIDED UNDER ARTICLE 11 AND
V.R.CR.P. 4134**

CONCLUSION36

CERTIFICATE OF COMPLIANCE.....37

TABLE OF AUTHORITIES

Cases

<u>Arizona v. Hicks</u> , 480 U.S. 321, 326 (1987).....	31
<u>Chimel v. California</u> , 395 U.S. 752 (1969).....	19
<u>City of Ontario, Cal. v. Quon</u> , 130 S. Ct. 2619, 2632 (2010).....	13
<u>Davis v. United States</u> , 328 U.S. 582, 603-05 (1946).....	19
<u>Douglas v. Windham Superior Court</u> , 157 Vt. 34, 38-39, 597 A.2d 774, 777 (1991).....	9
<u>Harris v. United States</u> , 331 U.S. 145, 157-62 (1947).....	19
<u>Horton v. California</u> , 496 U.S. 128, 136-137 (1990).....	31
<u>In re C.C.</u> , 2009 VT 108, ¶ 11, 186 Vt. 474, 480, 987 A.2d 1000, 1003.....	32
<u>In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621</u> , 321 F. Supp.2d 953, 961 (N.D. Ill. 2004).....	16
<u>Katz v. United States</u> , 389 U.S. 347, 351 (1967).....	33
<u>Lincoln v. Smith</u> , 27 Vt. 328, 347 (1855).....	20
<u>Marron v. United States</u> , 275 U.S. 192, 196 (1927).....	20
<u>New York v. Belton</u> , 453 U.S. 454 (1981).....	13
<u>Stanford v. Texas</u> , 379 U.S. 476, 485 (1965).....	20, 26
<u>State v. Badger</u> , 141 Vt. 430, 450 A.2d 336, (1982).....	12
<u>State v. Bauder</u> , 2007 VT 16, ¶¶ 10-11, 181 Vt. 392, 924 A.2d 38.....	12, 13, 35
<u>State v. Berard</u> , 154 Vt. 306, 310, 576 A.2d 118, 120 (1990).....	12
<u>State v. Birchard</u> , 2010 VT 57, 5 A.3d 879, 884-885.....	14
<u>State v. Blow</u> , 157 Vt. 513, 517, 602 A.2d 552, 555 (1991).....	13
<u>State v. Bryant</u> , 2008 VT 39, 183 Vt. 355, 361-362, 950 A.2d 467, 472.....	13
<u>State v. Connolly</u> , 133 Vt. 565, 570, 350 A.2d 364, 368 (1975).....	35
<u>State v. Crannell</u> , 170 Vt. 387, 394, 750 A.2d 1002, 1010 (2000).....	15
<u>State v. Crandall</u> , 162 Vt. 66, 69, 644 A.2d 320, 322-323 (1994).....	28, 29
<u>State v. Cunningham</u> , 2008 VT 43, 183 Vt. 401, 421, 954 A.2d 1290, 1302.....	14
<u>State v. Forte</u> , 154 Vt. 46, 48, 572 A.2d 941, 942 (1990).....	9
<u>State v. Geraw</u> , 173 Vt. 350, 353 n.2, 357-358, 795 A.2d 1219, 1222 n.2, 1225 (2002).....	13
<u>State v. Gray</u> , 150 Vt. 184, 189, 552 A.2d 1190, 1193 (1988).....	28, 29
<u>State v. Hill</u> , 459 F.3d 966, 978 (9th Cir. 2006).....	30
<u>State v. Kirchoff</u> , 156 Vt. 1, 13-14, 587 A.2d 988, 996-997 (1991).....	13
<u>State v. Martin</u> , 2008 VT 53, ¶ 10, 184 Vt. 23, 33 n.7, 955 A.2d 1144, 1150 n.7.....	21
<u>State v. Morris</u> , 165 Vt. 111, 125, 680 A.2d 90, 100 (1996).....	33, 35
<u>State v. Neil</u> , 2008 VT 79, 184 Vt. 243, 246, 958 A.2d 1173, 1176.....	14
<u>State v. Oakes</u> , 157 Vt. 171, 173, 598 A.2d 119, 121 (1991).....	19
<u>State v. Oney</u> , 2009 VT 116, ¶ 13. n.6, -- Vt. --, 989 A.2d 995, 999 n.6.....	35
<u>State v. Platt</u> , 154 Vt. 179, 185, 574 A.2d 789, 793 (1990).....	27
<u>State v. Pratt</u> , 173 Vt. 562, 563, 795 A.2d 1148, 1149 (2002).....	9
<u>State v. Quigley</u> , 2005 VT 128, ¶ 15, 179 Vt. 567, 571, 892 A.2d 211, 218.....	21, 27
<u>State v. Record</u> , 150 Vt. 84, 85, 548 A.2d 422, 423-424 (1988).....	10
<u>State v. Rogers</u> , 161 Vt. 236, 244, 638 A.2d 569, 573-574 (1993).....	33
<u>State v. Savva</u> , 159 Vt. 75, 616 A.2d 774 (1991).....	13, 14, 17, 19
<u>State v. Sprague</u> , 2003 VT 20, ¶ 17, 175 Vt. 123, 129-130, 824 A.2d 539, 545.....	21
<u>State v. Towne</u> , 158 Vt. 607, 616, 615 A.2d 484, 489 (1992).....	27
<u>State v. Trudeau</u> , 165 Vt. 355, 358, 683 A.2d 725, 727 (1996).....	31
<u>State v. Wood</u> , 148 Vt. 479, 487, 536 A.2d 902, 907 (1987).....	12
<u>United States v. Abbell</u> , 963 F. Supp. 1178, 1199 (S.D. Fla 1997).....	30
<u>United States v. Banks</u> , 540 U.S. 31, 36 (2003).....	15
<u>United States v. Bedford</u> , 519 F.2d 650, 655 (3d Cir. 1975).....	15
<u>United States v. Brunette</u> , 76 F. Supp. 2d 30, 42 (D. Me. 1999).....	15
<u>United States v. Carey</u> , 172 F.3d 1268, 1273 (10th Cir. 1999).....	32
<u>United States v. Chaidez</u> , 919 F.2d 1193, 1197 (7th Cir. 1990).....	28

<u>United States v. Comprehensive Drug Testing, Inc.</u> , 621 F.3d 1162, 1178 (9th Cir. 2010).....	29
<u>United States v. Leon</u> , 468 U.S. 897 (1984).....	19
<u>United States v. Rabinowitz</u> , 339 U.S. 56, 66 (1950)	19
<u>United States v. Ricciardelli</u> , 998 F.2d 8, 12 (1st Cir. 1993)	16
<u>United States v. Ross</u> , 456 U.S. 798, 829 (1982).....	17
<u>United States v. Rowland</u> , 145 F.3d 1194, 1201-1202 (10th Cir. 1998).....	16
<u>United States v. Santore</u> , 290 F.2d 51, 67 (2d Cir. 1960)	21
<u>United States v. Shegog</u> , 787 F.2d 420, 422 (8th Cir. 1986).....	16
<u>Walter v. United States</u> , 447 U.S. 649, 653 (1980).....	23, 26, 32
 <u>Statutes</u>	
13 V.S.A. § 2030.....	6
 <u>Rules</u>	
V.R.Cr.P. 41.....	passim
 <u>Other Authorities</u>	
Orin S. Kerr, <u>Digital Evidence and the New Criminal Procedure</u> , 105 Colum. L. Rev. 279, 290 (2005)....	23, 25
Paul Ohm, <u>The Myth of the Superuser: Fear, Risk, and Harm Online</u> , 41 U.C. Davis L Rev. 1327, 1355 (2008).....	30
Susan W. Brenner and Barbara A. Frederiksen, <u>Computer Searches and Seizures: Some Unresolved Issues</u> , 8 Mich. Telecomm. & Tech. L. Rev. 39, 94-95 (2002).....	32, 33, 34
 <u>Treatises</u>	
2 W. LaFave, <u>Search & Seizure</u> § 3.2(e).....	27
 <u>Constitutional Provisions</u>	
Vt. Const. ch. 1, art. 11	passim
U.S. Const. amend IV	passim

STATEMENT OF THE FACTS

The State has filed a petition for extraordinary relief under V.R.A.P. 21 (b) requesting this Court to strike the conditions ordered by the lower court when it issued a warrant to search the residence of 145 Pleasant Avenue, Burlington, Vermont for evidence of the suspected crime of identity theft under 13 V.S.A. § 2030. Because the State has not arrested any person associated with this alleged crime, there is no defendant or opposing party to the State's petition. The Office of the Defender General submits this brief in opposition to the State's brief as amicus curiae.

The State seeks to search and seize the following objects and possessions from 145 Pleasant Avenue:

Any correspondence...electronic mail, chat logs, electronic documents, diaries, notebooks, notes, address books, mailing lists, address labels, or other documents pertaining to...[d]ominion 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....

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 (hereafter "MEDIA") that were or may have been used as a means to commit the offenses described on the warrant.

...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...passwords, encryption keys, and other access devices that may be necessary to access the MEDIA.

P.C. 14.

In support of this warrant application, the State attached an affidavit by Detective Warren. P.C. 7. The affidavit served as the only evidence of probable cause for the warrant.

In the warrant application, the Detective asserted that someone had filed a change of address form on behalf of Mr. John Kacur without Mr. Kacur's permission. The new address listed was 145 Pleasant Avenue, Burlington, Vermont. P.C. 8. Mr. Kacur resided in upstate New York. Mr. Kacur told the detective that three attempts were made to obtain credit cards under his name. Id. The Detective learned from the First National Bank of Omaha that an attempt to obtain a visa card under Mr. Kacur's name occurred on July 16, 2010. The detective also learned that this transaction was done over the internet and completed at 8:56 a.m. utilizing an IP address of 24.91.163.40. Id. The email address of gulfields@aol.com was listed on the application form.

The subscriber of the IP address was Barbara Strong, an internet user who resided at 134 Pleasant Avenue, Burlington, Vermont, located "diagonally across the street within approximately 100 feet" from 145 Pleasant Avenue. Ms. Strong told the detective "that she was in no way involved in any fraudulent applications for credit cards" and that she did not know Mr. Kacur or anyone from upstate New York. P.C. 9. Ms. Strong admitted to the detective that she lived alone, was a high school teacher, and had three children attending college in California, Wyoming, and Utah. In December 2010, she told the detective that her children had previously resided with her, but that they had left home at the beginning of the school year. The search warrant does not target Ms. Strong or any of her three children.

In December 2010, the detective learned that Ms. Strong had an open wireless internet connection. The detective claimed that "[i]t appeared that the

signal was strong enough to access from 145 Pleasant Avenue.” When the detective checked Ms. Strong’s router logs to learn who accessed her wireless internet, he saw that a computer with the assigned name of GulfieldProp-PC accessed the account on multiple occasions during the month of November 2010. P.C. 10.

There was no evidence that a computer located at 145 Pleasant Street accessed Ms. Strong’s IP address in July 2010, the month when the alleged fraudulent credit card application was submitted over the internet. The detective’s affidavit provided no details concerning the other two attempts to apply for credit cards except to establish that they involved a Citi Card and a Kohl’s/Chase card. P.C. 8. There was no information as to when these other attempts were made or that these attempts involved the residence of 145 Pleasant Avenue. There was also no evidence submitted as to when the change of address notice was filed or whether the form was submitted over the internet or by physical mail.

The detective confirmed that 145 Pleasant Avenue was occupied by Eric Gulfield, but he also confirmed that “more than one person resides at the PREMISES [sic].” P.C. 8, 11. No other residents of 145 Pleasant Avenue were named in the affidavit. The subsequent request for a warrant to search all media at the residence was justified by the detective’s assertion that criminals can hide data and “may try to conceal criminal evidence.” P.C. 12. After the court amended the State’s proposed warrant to include several conditions restricting the scope of the search of “Mr. Gulfield’s computer,” it found sufficient probable cause and issued the warrant. P.C. 1-2. While the judge identified the computer to be searched as

belonging to Mr. Gulfield, P.C. 3, there was no evidence that there was only one computer to be seized or that any of the electronic devices that might be found at the residence belonged to Mr. Gulfield.

The court ordered the State to provide a return disclosing precisely what data was obtained by the search of the computer “[w]ithin the time specified in the warrant,” P.C. 4. However, no deadline for executing the search or for filing a return was set in the warrant. The State remains in possession of the computer and asserts that it has not conducted a search of the electronic device. State’s brief at 3.

STANDARD OF REVIEW

Review of a petition for extraordinary relief is of “very limited scope.” Douglas v. Windham Superior Court, 157 Vt. 34, 38-39, 597 A.2d 774, 777 (1991). Unless the Court determines that the judge could not as a matter of discretion order the warrant conditions, it should not disturb the ruling, even if it disagrees with its judgment. State v. Forte, 154 Vt. 46, 48, 572 A.2d 941, 942 (1990). The requirements for a petition for extraordinary relief are twofold. The State must show that it has no other avenue of relief, and that the judge’s decision constitutes a usurpation of judicial authority or clear abuse of discretion. State v. Pratt, 173 Vt. 562, 563, 795 A.2d 1148, 1149 (2002). To show usurpation of judicial power, the State is required to establish more than that the trial court was wrong or gave the wrong reason for its action. Douglas, 157 Vt. at 39, 597 A.2d at 777. The State has the burden of proving that the lower court acted in “an arbitrary abuse of power.” Forte, 154 Vt. at 48, 572 A.2d at 942. “Clear abuse of discretion” has been

interpreted by the Court as requiring the State to show that the judge's decision "must be wrong as a matter of law." Id.

ARGUMENT

The State makes repeated claims throughout its brief that the court created a new legal framework without any authority when it imposed conditions on a search warrant having the effect of limiting the scope of a computer search. State's brief at 5-10, 12, 25. The ordering of these conditions; however, was not a rogue act but an act well within the judge's discretion to make to ensure that the sought after warrant did not become a general warrant, the absolute prohibited evil which Article 11 protects against. State v. Record, 150 Vt. 84, 85, 548 A.2d 422, 423-424 (1988). It is under the long-standing legal framework of Vermont's Article 11 jurisprudence and the Rules of Criminal Procedure that the judge exercised his authority and followed his duty as a judicial officer to uphold the laws of Vermont to protect the privacy rights of Vermonters. The conditions imposed merely complied with the particularity and probable cause requirements of the Fourth Amendment, Article 11, and the Rules of Criminal Procedure 41. The court's restriction of the use of the plain view doctrine here was also a straightforward application of the Court's caselaw addressing this narrow exception to the warrant requirement.

Rather, it is the State who makes the radical argument for an entirely new framework for analyzing the search and seizure of electronic media found in the home, unmoored from the Fourth Amendment, Article 11 and the Rules of Criminal Procedure. The State argues for a criminal justice system where Article 11 rights are merely remedial and exerted at the suppression hearing to the select few who are charged with criminal offenses, leaving innocent parties who are never criminally charged without recourse to

challenge violations of their constitutional rights. State's brief 12-13. The State's argument is also a call to collapse the warrant requirement of probable cause and particularity into one of only reasonableness, with the standard of reasonableness linked not to the warrant requirement, but to a review of the conduct of law enforcement at the time of the search and seizure. *Id.* at 24. Finally, the State argues for application of the plain view doctrine here, but ignores long-standing precedent and the necessary prerequisites that must be found before this narrow exception to the warrant requirement is triggered. *Id.* at 21-22. The State's claim that the plain view doctrine applies in the context of electronic media searches would transform this warrant into the functional equivalent of a general warrant in direct contravention to Article 11.

The State raises several novel questions of first impression for this Court. The key question for purposes of this petition is whether the warrant-issuing judge had the discretion to impose the kinds of conditions ordered here. Implicit in this is the question of the degree of particularity and probable cause required to justify intrusion into a person's substantial privacy interests in the data stored on his or her computer or other electronic media in the home and the amount necessary to sufficiently limit police discretion when searching these devices. Another issue implicated is whether the plain view doctrine applies in the cyber-digital world.

The State's answers to these questions have far-reaching implications. Modern day reality is that of increasing dependence on computers and other electronic media for almost every aspect of our personal and professional lives. The increasing dependence on technology is propelled by the ever expanding capacities and capabilities of these devices to store and process more data. If the police and prosecutors are permitted to scour and

view all possible data contained within this media without limitation, the core protection of Article 11 against excessive government invasion is obliterated. The State's arguments here are nothing less than an appeal to this Court to fundamentally erode the Vermont Constitution. Because the judge was well within his discretion to order these conditions and because the State fails to make any argument how it has no other avenue of relief, the Court should deny the State's petition.

I. THE WARRANT-ISSUING JUDGE HAS AUTHORITY TO IMPOSE ANY REASONABLY APPROPRIATE CONDITIONS TO ENSURE THAT THE WARRANT IS IN FULL COMPLIANCE WITH ARTICLE 11 OF THE VERMONT CONSTITUTION AND THE RULES OF CRIMINAL PROCEDURE

A. Article 11 jurisprudence requires more exacting judicial oversight than does the Fourth Amendment

The Court has long held that Vermont's "values of privacy and individual freedom—embodied in Article 11—may require greater protection than that afforded by the federal Constitution." State v. Bauder, 2007 VT 16, ¶¶ 10-11. 181 Vt. 392, 924 A.2d 38. Since the Court's landmark decision in State v. Badger, 141 Vt. 430, 450 A.2d 336, (1982) the Court has repeatedly interpreted Article 11 as requiring broader and more demanding judicial oversight than that required by the Fourth Amendment. State v. Wood, 148 Vt. 479, 487, 536 A.2d 902, 907 (1987) (noting that in focusing away from judicial review and curtailing scope of protected right to be free from unlawful governmental conduct, federal law is incompatible with Article 11); State v. Berard, 154 Vt. 306, 310, 576 A.2d 118, 120 (1990) (recognizing that federal law "tends to derogate the central role of the judiciary in Article Eleven jurisprudence").

This departure from federal precedent has been particularly evident in two areas. First, the Court has parted company with federal precedent in its emphasis on the

requirement of a warrants, and the judicial supervision of searches and seizures which the warrant requirement is intended to secure. See e.g., Bauder, 2007 VT 16, ¶¶ 15-20, 181 Vt. 392, 924 A.2d 38 (refusing to adopt holding in New York v. Belton, 453 U.S. 454 (1981), that officers may routinely search automobiles and containers in them incident to arrest irrespective of need to assure safety or protect evidence); State v. Savva, 159 Vt. 75, 616 A.2d 774 (1991) (prohibiting officers from searching closed containers whose contents are not in plain view following automobile stop, and refusing to adopt Supreme Court caselaw not requiring particularized showing of exigent circumstances to search automobiles following stop); State v. Kirchoff, 156 Vt. 1, 13-14, 587 A.2d 988, 996-997 (1991) (warrant required for search of posted “ open fields”); State v. Bryant, 2008 VT 39, 183 Vt. 355, 361-362, 950 A.2d 467, 472 (aerial surveillance); State v. Blow, 157 Vt. 513, 517, 602 A.2d 552, 555 (1991) (electronic transmission of suspect’s conversation with police agent, from inside suspect’s home); State v. Geraw, 173 Vt. 350, 353 n.2, 357-358, 795 A.2d 1219, 1222 n.2, 1225 (2002) (police recording of such conversations).

B. Vermont’s “Least Intrusive Means” Requirement

A second respect in which Vermont’s Article 11 jurisdiction parts company with the Fourth Amendment is on the question whether searches and seizures must be conducted by the least intrusive means available.

The United States Supreme Court has made abundantly clear that a search may pass muster under the Fourth Amendment even if it is not conducted by the least intrusive or restrictive means available. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2632 (2010) (“This Court has “repeatedly refused to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment.”) (citing cases). This

Court has made it equally clear, in a long line of Article 11 cases, that searches and seizures must be conducted by the least intrusive means. With respect to containers,

Even where probable cause exists to seize a closed container, that does not override the requirement for a warrant: police must proceed in the least intrusive manner with respect to a defendant's expectations of privacy in that container....

State v. Birchard, 2010 VT 57, 5 A.3d 879, 884-885. See e.g., State v. Cunningham, 2008 VT 43, 183 Vt. 401, 421, 954 A.2d 1290, 1302 (investigative detentions); State v. Neil, 2008 VT 79, 184 Vt. 243, 246, 958 A.2d 1173, 1176 (same); Savva, 159 Vt. at 88-89, 616 A.2d at 781 (demanding that, when acting without a warrant, police operate “in the least intrusive manner possible under the circumstances”).

C. Vermont Courts Have Recognized Authority to Regulate the Manner in Which a Search May be Conducted.

The State makes a broad and entirely untenable proposition that warrant-issuing judges in Vermont may only approve or disapprove a warrant application, and that they lack any authority to regulate the manner in which the search may be conducted. The language of the Fourth Amendment

empowers a judicial officer in reviewing a search warrant to ensure that the affidavit establishes probable cause and that the warrant specifies the place to be searched and the persons or things to be seized. This language, however, does not authorize the judicial officer to otherwise dictate how law enforcement must conduct the search...

State's brief at 6. The same is true, the State adds, of Article 11, and V.R.Cr.P. 41. Id. 8-10.

In fact Vermont judges, as well as judges elsewhere in the United States, have long been authorized to address how a search may be conducted, not simply whether it

may be conducted at all. For example, in the case of a home search, the judge may choose to issue a “knock and announce” warrant or, in appropriate cases, a no-knock warrant. See State v. Crannell, 170 Vt. 387, 394, 750 A.2d 1002, 1010 (2000); United States v. Banks, 540 U.S. 31, 36 (2003) (“When a warrant applicant gives reasonable grounds to expect futility or to suspect that one or another such exigency already exists or will arise instantly upon knocking, a magistrate judge is acting within the Constitution to authorize a “no-knock” entry.”). The Fourth Amendment and Article 11 are silent about both these options, but no one can doubt that issuing judges have discretion to choose one or the other.

Neither the Fourth Amendment nor Article 11 specifies when a warrant must be executed. Rule 41 does: police must “serve the warrant within a specified period of time not to exceed 10 days from issuance....” V.R.Cr.P. 41 (c)(5)(A)(i). See United States v. Brunette, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (suppressing evidence not reviewed within the time period set forth in the warrant and extension granted); United States v. Bedford, 519 F.2d 650, 655 (3d Cir. 1975) (upholding imposition of time limits because “[i]f 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”).

Neither the Fourth Amendment nor Article 11 specifies the time of day when a warrant must be executed. Rule 41 does: “between the hours of 6:00 A.M. and 10:00 P.M. unless the judicial officer for reasonable cause shown authorizes execution at other times....” V.R.Cr.P. 41 (ii).

Neither the Fourth Amendment nor Article 11 specifies the amount of time that

may lapse after execution of a warrant and before its return. Rule 41(d)(1) requires that it be done “promptly.” The application in this case asked “permission to take as long as necessary” to examine the seized devices and media. P.C. 13.

Issuing magistrates are also permitted, in their discretion, to make execution of a warrant contingent on a future event. United States v. Shegog, 787 F.2d 420, 422 (8th Cir. 1986). See also United States v. Rowland, 145 F.3d 1194, 1201-1202 (10th Cir. 1998) (holding that a condition precedent is necessary for an anticipatory warrant because it “not only insures against premature execution of the warrant, but also maintains judicial control over the probable cause determination and over the circumstances of the warrant's execution.”) (citations omitted); United States v. Ricciardelli, 998 F.2d 8, 12 (1st Cir. 1993) (noting the need to place limits on anticipatory warrants to prevent possible abuse). See also Brief Amicus Curiae of the American Civil Liberties Union Foundation of Vermont, et al., 10-11 (citing cases approving ex ante appointment of special masters). The State’s argument “that a judge is powerless to regulate the means of executing a search and seizure is belied by the government’s own request in this case that the court approve one particular method of executing the search...” In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621, 321 F. Supp.2d 953, 961 (N.D. Ill. 2004).

The issue is not, as the State maintains, whether the issuing judge had authority to impose ex ante conditions on the requested searches. He clearly did. The question before this Court is not one of judicial authority, but judicial discretion. Has the State carried the burden of showing that the judge abused his discretion in imposing the

conditions at issue? Amicus contends that the conditions were eminently reasonable and appropriate, given the scope and intrusiveness of the proposed search.

II. THE STATE'S CLAIM THAT JUDICIAL REVIEW AT THE SUPPRESSION HEARING AND AN OVERALL STANDARD OF REASONABLENESS IS SUFFICIENT PROTECTION OF PRIVACY RIGHTS CONTRAVENES VERMONT LAW

The State seems to concede the possibility of abuse, and proposes a solution: although the warrant-issuing judge may not impose *ex ante* conditions in the warrant, the fruits of the search may be suppressed pursuant to a motion to suppress, on a post-hoc finding that the search, or the manner in which police conducted it, was “unreasonable.” State’s brief at 12-13 The State’s proposal is a “solution” only if the Court is willing to accept a future in which innocent people, not charged with any crime, lack any enforceable privacy interest in their electronics, and only if the Court consigns people who are charged with criminal conduct to a Fourth Amendment “reasonableness” rule which the United States Supreme Court rejected more than half a century ago.

A. Post-hoc judicial review, by motion to suppress, offers no protection for computer-users who have not been suspected of or charged with any crime

State v. Savva addressed this very issue.

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.”

159 Vt. at 86 (emphasis added) (citing United States v. Ross, 456 U.S. 798, 829 (1982). (Marshall, J., dissenting)).

One need not look far for an example of a presumably law-abiding citizen with no remedy for an unconstitutional search. The search warrant application in this case

requests the right to seize and search all computers and electronic media found at 145 Pleasant Ave., even though some of the computers may belong to non-suspects.

“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.” P.C. 11 ¶ 8. “[P]redominantly used” is something of a euphemism: the requested warrant covers computers and media that are owned and *exclusively* used by non-suspects.

In effect, the State is boldly asserting an unreviewable power to sift through the private lives of citizens who are not suspected of any crime, who are not charged with any crime, and whose computers were never suspected of containing any contraband or criminal evidence except on the flimsiest grounds: their proximity to computers and media which were suspect. This system cannot coexist with Article 11’s privacy guarantee. It also violates Ch. I, art. 4 of the Vermont constitution, which guarantees that “[e]very person within this state ought to find a certain remedy, by having recourse to the laws, for all injuries or wrongs which one may receive in person, property or character....”

B. The State’s post-hoc “reasonableness” standard provides no realistic remedy to persons charged with crime.

The State argues that the court’s conditions on the warrant have “no legal effect” as the “ultimate measure of the constitutionality of the search is reasonableness.” State’s brief at 24, 25.

Insofar as the State proposes this post-hoc review under the Fourth Amendment, the remedy is entirely illusory. The fruits of computer searches, undertaken under the sort of warrant the State is asking for, will be admissible so long as the police have acted

in good faith. United States v. Leon, 468 U.S. 897 (1984). Reasonableness in this context boils down to whether the police had reasonable grounds for believing that the warrant was properly issued. *Id.* at 919-920. If the State's scheme is accepted, such open-ended warrants will *always* be "reasonable" and their fruits will *never* be suppressible.

Article 11 is not subject to the same Catch-22. See State v. Oakes, 157 Vt. 171, 173, 598 A.2d 119, 121 (1991) (rejecting "good faith" exception). But the State's proposed "reasonableness" rule raises other grave difficulties.

In decisions handed down in the 1940s and '50s the United States Supreme Court vacillated between an unadorned rule of "reason" permitting wide ranging warrantless searches, and a presumption in favor of warrants, whenever practicable. An example of the former approach is United States v. Rabinowitz, 339 U.S. 56, 66 (1950) where the Court concluded that the test of a search "is not whether it is reasonable to procure a search warrant, but whether the search was reasonable." That permissive approach was laid to rest by Chimel v. California, 395 U.S. 752 (1969), which discusses and rejects the line of cases of which Rabinowitz is a part. *Id.* at 755-760.

State v. Savva discusses some of the same cases, stressing Justice Frankfurter's dissents in Rabinowitz and two other cases in the Rabinowitz line, Davis v. United States, 328 U.S. 582, 603-05 (1946), and Harris v. United States, 331 U.S. 145, 157-62 (1947). 159 Vt. at 85, 616 A.2d at 779-780. Frankfurter's Rabinowitz dissent speaks directly to this case.

The purpose of the Fourth Amendment was to assure that the existence of probable cause as the legal basis for making a search was to be determined by a judicial officer before arrest and not after, subject only to what is necessarily to be excepted from such requirement. The exceptions cannot be enthroned into the rule. The

justification for intrusion into a man's privacy was to be determined by a magistrate uninfluenced by what may turn out to be a successful search for papers, the desire to search for which might be the very reason for the Fourth Amendment's prohibition.

339 U.S. at 80. The State's post-search "rule of reason" is nothing more than a variation on the rule which Justice Frankfurter in dissent, and subsequent cases by their holdings, have unambiguously rejected. Judging the lawfulness of computer searches after the fact, rather than regulating them ex ante, violates Article 11's presumption in favor of warrants.

III. THE COURT'S CONDITIONS WERE WELL WITHIN ITS DISCRETION TO IMPOSE IN ORDER TO SATISFY PARTICULARITY REQUIREMENTS UNDER VERMONT LAW AND TO AVOID A GENERAL WARRANT

A. Article 11 requires that particularity be sufficiently detailed to avoid a general warrant and unchecked discretion by the government

To prevent against the issuance and enforcement of general warrants, Article 11 requires particularized suspicion to justify a search or seizure of a person's possessions. Vt. const. ch. I, art. 11; Record, 150 Vt. at 85, 548 A.2d at 423-424. The Court has interpreted this to mean that property searched and seized should be described "as nearly as may be." Lincoln v. Smith, 27 Vt. 328, 347 (1855). The United States Supreme Court requires sufficient particularity such that no discretion is left to the officer executing the warrant. Marron v. United States, 275 U.S. 192, 196 (1927). The particularity requirement prevents against warrants supported by probable cause turning into general warrants. Stanford v. Texas, 379 U.S. 476, 485 (1965). The Court has recognized that "[t]he most common meaning of 'general warrant' was a warrant that lacked specificity

as to whom to arrest or where to search; for example, a warrant directing ... a search of suspicious places.” State v. Martin, 2008 VT 53, ¶ 10, 184 Vt. 23, 33 n.7, 955 A.2d 1144, 1150 n.7 (internal quotations and citation omitted).

The requirement of particularity encompasses the fundamental principle that any government intrusion into a person’s Article 11 rights should proceed no further than necessary to effectuate the purpose of the warrant. See Birchard, 2010 VT 57, ¶ 13, 5 A.3d at 885; State v. Sprague, 2003 VT 20, ¶ 17, 175 Vt. 123, 129-130, 824 A.2d 539, 545 (discussing that implicit in the rule authorizing police to stop and detain vehicles based on reasonable suspicion “is the corollary requirement that the police intrusion proceed no further than necessary to effectuate the purpose of the stop”).

The Court has declined to interpret Article 11’s particularity requirements as being simply co-extensive with the Fourth Amendment. State v. Quigley, 2005 VT 128, ¶ 15, 179 Vt. 567, 571, 892 A.2d 211, 218. The Court has not recognized the “community living” exception to the particularity requirement under Article 11, an exception long accepted by the Second Circuit and other courts under the Fourth Amendment. Id. (citing United States v. Santore, 290 F.2d 51, 67 (2d Cir. 1960)).¹

If the underlying principle of Article 11 is that the police must employ the least intrusive means to avoid unnecessary invasions of privacy, then the particularity required must be more than merely identifying the targeted electronic media to be searched. See

¹ The community living exception under the Fourth Amendment applies only where the police could not have known that they would encounter separate privacy interests inside the premises prior to executing the search warrant. Quigley, 2005 VT 128, ¶ 17, 179 Vt. at 571-572, 892 A.2d at 218. As the detective here readily admitted in the affidavit that there were several people residing at 145 Pleasant and that the officer expected that innocent third parties may own or predominantly use the same electronic media targeted, the exception to the particularity clause under the Fourth Amendment does not apply. P.C. 25; see Quigley, 2005 VT 128, ¶ 17, 179 Vt. at 571-572, 892 A.2d at 218.

e.g., Savva, 159 Vt. at 90, 616 A.2d at 782. Such a bare bones list fails to identify the media search “as nearly as may be.” Lincoln, 27 Vt. at 347. It also falls far short of eliminating police discretion.

B. V.R.Cr.P. 41 sets a high standard for particularity in the warrant

The Criminal Rules of Procedure likewise require a high degree of particularity.

V.R.Cr.P. 41 provides:

If the judicial officer is satisfied that there is probable cause to believe that grounds for the application exist, he shall issue a warrant identifying the property or other object of the search and naming or describing the person or place to be searched.

V.R. Cr.P. 41 (c).

Under the rule, before the court can issue a warrant it must identify “the property or other object of the search.” V.R.Cr.P. 41 (c). The high degree of particularity required by this phrase is established by how the rule defines the term “property.” The rule defines it as including “documents, books, papers, and any other tangible objects[.]” V.R.Cr.P. 41 (h). Inserting this definition into V.R.Cr.P. (c), the judge is required to “identify” the documents, papers, and any other tangible objects “or other object of the search and nam[e] or describe[e] the...place to be searched.” The language of the rule makes clear that all tangible and intangible objects must be identified with sufficient detail equivalent to at least the paper, document or book, and the place named or described. The level of detail demanded by Rule 41 was clearly not met by the State’s proposed warrant where no electronic records, documents, files, types of files, or dates of files were listed.

C. A wholesale search of all electronic devices is the functional equivalent of a general warrant and captures protected communications under the First Amendment

The fundamental problem with the State's warrant application is that it seeks a wholesale search and seizure of the entire contents of all electronic media found at the home without restriction. P.C. 10-13. However, "exploratory searches...cannot be undertaken by officers with or without a warrant..." Walter v. United States, 447 U.S. 649, 653 (1980) (quotations omitted). For the Court to uphold the State's proposed warrant "is to invite a government official to use a seemingly precise and legal warrant only as a ticket to get into a man's home, and, once inside, to launch forth upon unconfined searches and indiscriminate seizures as if armed with all the unbridled and illegal power of a general warrant." Id.

Existing search and seizure caselaw is "naturally tailored to the facts of physical-world crimes." Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279, 290 (2005). Applying this caselaw to digital searches may require new and additional considerations; however, a completely new legal framework is unwarranted. When the capacities and capabilities of electronic media are made analogous to objects found in the physical world, it becomes clear that wholesale searches of these devices are the modern day equivalent of the general warrant.

A typical personal computer sold in 2011 may have a 500 gigabyte hard drive. See "How to Buy a Desktop PC," <http://www.pcmag.com/article2/0,2817,2357400,00.asp> (last visited June 16, 2011). In physical and comparative terms, the hard drive of a typical new home computer in 2005 "stored at least forty gigabytes of information, roughly equivalent to twenty million pages of text or about half the information stored in the books located on one floor of a typical academic library." Kerr, *supra* at 302. Practically speaking, such hard drives are filled not

only with intentionally stored documents, but also with cookies, cache files, browser histories, and index files that quietly document the web pages accessed on the computer, the logins and passwords of the users of the computer, and the actions taken at various websites. See “How to Reclaim Your Online Privacy,” PC Magazine Online, <http://www.pcmag.com/article2/0,2817,2334782,00.asp> (last visited June 16, 2011). Even when such files are deleted, they are often still easily recoverable. See “Deleting May Be Easy, but Your Hard Drive Still Tells All”, <https://www.nytimes.com/2006/04/05/technology/techspecial4/05forensic.html?scp=1&sq=Deleting%20May%20Be%20Easy,%20but%20Your%20Hard%20Drive%20Still%20Tells%20All&st=cse> (last visited June 16, 2011). Increased connectivity amongst computers further complicates digital searches. Home computers, work computers, and even cell phones are likely to be linked to the same networked storage media, allowing seamless access to tremendous amounts of data from any of a number of digital devices. See “Data Grows, and So Do Storage Sites” <https://www.nytimes.com/2011/06/06/technology/internet/06dropbox.html?scp=2&sq=Data%20Grows,%20and%20So%20Do%20Storage%20Sites&st=Search> (last visited June 16, 2011). A federal district court, struck by the constitutional significance of the interactive nature of electronic media, found that “digital devices are not just repositories of data, but access points, or portals, to other digital devices and data, typically obtained through the internet or stored on a network. The requested warrant is, in essence, boundless.” In the Matter of the United States of America’s application for a search warrant to seize and search electronic devices from Edward Cunnius, -- F. Supp. 2d --, 2011 WL 991405, *6 (W.D. Wash. 2011).

Though the State seeks to treat digital search warrants as they would a warrant for a physical search of a box or file cabinet, P.C. 23, such analogies are inadequate. Unlike a file cabinet, which may contain tens or hundreds of files, a computer is likely to contain hundreds of thousands of individual files. Unlike a file cabinet, which contains files purposefully stored by its user, the bulk of the information on a hard drive is not intentionally stored by the user and often has been deleted. Professor Orin Kerr proposed that a more appropriate analogy for the search of a “typical home computer,” which at the time “stored at least forty gigabytes of information” was “something like limiting a search to a city block.” Kerr, supra at 303. He went on to note that “ten years from now, it will be like limiting a search to the entire city.” Id.

As digital storage capacity and connectivity has increased, its use for sensitive communication and data storage has become commonplace. An unconstrained digital search of a home computer, like the one requested in this case, is likely to expose medical records, personal communications, private photographs, a digital library, financial information, purchase records, and dating profiles. See e.g., “Breaches Lead to Renewed Effort to Protect Medical Data”

<http://www.nytimes.com/2011/05/31/business/31privacy.html?ref=privacy> (last visited June 16, 2011); “Sexting Not Just for Kids” http://www.aarp.org/relationships/love-sex/info-11-2009/sexting_not_just_for_kids.html (last visited June 16, 2011).

In many cases, such a search may also implicate expressive material subject to heightened application of search and seizure protections. The ubiquity of personal computers, cellular phones, and digital cameras has turned ordinary citizens into very effective journalists. See e.g., “What We Need for a Local Reporting Renaissance,”

<http://www.theatlanticwire.com/business/2011/06/local-reporting-patch-aol-citizen-journalism/38664/> (last visited June 16, 2011). Just as home computers have been turned into tools of journalism, they have also become tools of political organization and mobilization. See generally Richard Kahn and Douglas Kellner “Oppositional Politics and the Internet” *Cultural Politics: An International Journal*, March 2005 75-100. A warrant allowing the wholesale search of a personal computer, including the exposure of these kinds of presumptively protected materials under the First Amendment must be highly constrained. Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1970) (“Where presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field.”); Stanford v. Texas, 379 U.S. 476, 482 (1965) (where warrant authorized rummage through books and papers making judgments about each item examined, it was the functional equivalent of a general warrant). It is the requirement that the warrant particularly describe the things to be seized that “makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.” Walter, 447 U.S. at 657, n. 7 (1980) (quoting Marron, 275 U.S. at 196).

The State tries to reassure the Court that the search is not excessive because no innocent third-party privacy interests are implicated. State’s brief at 13, 19. But this assertion is directly contrary to the detective’s statements in the affidavit, which establish that other people residing at 145 Pleasant Avenue, who are not suspected of committing any crime, may own, exclusively use, or predominately use the electronic media targeted by the police search. P.C. 25. The judge’s imposed conditions constituted an entirely

proper exercise of his discretion to uphold the particularity requirements of the warrant under Vermont law.

IV. THE COURT'S CONDITIONS WERE WELL WITHIN ITS DISCRETION TO IMPOSE TO ENSURE THAT THERE WAS PROBABLE CAUSE TO SUPPORT THE SEARCH OF THE COMPUTER

Before a search warrant can be issued, the State must show that there is probable cause based upon substantial evidence that “a person of reasonable caution would conclude that a crime has been committed and that evidence of the crime will be found in the place to be searched.” State v. Platt, 154 Vt. 179, 185, 574 A.2d 789, 793 (1990). “Although the police may have probable cause that a suspect committed a particular crime, they will not always have probable cause to search “all places over which that individual exercises control.” State v. Towne, 158 Vt. 607, 616, 615 A.2d 484, 489 (1992). Where the probable cause to search implicates the privacy rights of third parties, Justice Dooley held, “[W]e should be more hesitant to find probable cause in searches of multiple places, controlled by different persons, where a serious risk of invading the privacy of an innocent person exists.” Quigley, 2005 VT. 128, ¶ 28, 179 Vt. at 576, 892 A.2d at 222 (Dooley, J., concurring) (citing 2 W. LaFare, *Search & Seizure* § 3.2(e), at 78-84 (4th ed. 2004)).

The State concedes that “the search of an entire computer owned and operated by a third-party not involved in the crime” would not be justified by the detective’s assertion in the affidavit that “suspects often attempt to conceal incriminating computer files.”² State’s brief 13. However, the detective confirms just this when he admits in the affidavit

² The State misstates the detective’s claim. The detective did not assert that suspects “often” attempt to conceal files. State’s brief 13. Instead,, the detective used even more generic and vague language: “a suspect may try to conceal criminal evidence” and “[c]riminals can mislabel or hide files....” P.C. 12.

that third-parties may own or predominantly use the media targeted by the search. P.C. 12.

Additionally, the evidence that electronic media at 145 Pleasant Avenue was used in the alleged crimes is scant at best. Although the detective claimed multiple instances of identify theft to acquire three credit cards, the affidavit links 145 Pleasant Avenue to only one single incident. This information, gleaned from the First National Bank of Omaha, revealed that on July 16, 2010 at 8:56 a.m. someone with the IP address of 24.91.163.40 completed a transaction for a credit card over the internet. The application showed an email address of gulfields@aol.com and a residential address of 145 Pleasant Avenue. There were no other details as to when, where, or who were involved in the other two allegations of credit card fraud or whether these incidents were done over the internet or submitted by mail. Similarly, there was no evidence that electronic media was used in the filing of the change of address form.

The underlying issue here is “whether there [i]s adequate justification for each of the increasingly greater intrusions” sought by the police into all electronic data contained on all electronic media found in 145 Pleasant Avenue. State v. Crandall, 162 Vt. 66, 69, 644 A.2d 320, 322-323 (1994) (citing United States v. Chaidez, 919 F.2d 1193, 1197 (7th Cir.1990) (continuum of stricter requirements must be established to justify increasingly greater intrusions); State v. Gray, 150 Vt. 184, 189, 552 A.2d 1190, 1193 (1988) (to same effect)). There was not. At most the evidence supported probable cause to search for electronic records relating to credit card fraud occurring in one distinct moment in time: at 8:56 a.m. on July 16, 2010. However, the State’s proposed warrant was not restricted by date or to files relating to credit card records, or even to electronic records relating to

change of address forms. Instead, it sought authorization to search and seize any and all electronic data on all electronic media. The limited evidence presented to the judge failed to support the warrant's probable cause requirements necessary to avoid an overbroad search.

The State's application for a search warrant further shows that the police anticipated that there would be areas within the electronic media that would contain inaccessible data separately secured by way of encryption, deletion, or password protection. P.C. 14. The affidavit for probable cause, however, fails to account for the various privacy interests reflected by the special treatment of this type data on the computer. Instead, the warrant application merely provides a general description of electronic devices as the place or object to be searched as set by its outward appearance and without regard to the separate and heightened privacy interests contained therein in derogation of the law. Crandall, 162 Vt. at 69, 644 A.2d at 322-323; Gray, 150 Vt. at 189, 552 A.2d at 1193. The judge's conditions relating to segregating electronic data was the mechanism to ensure that the State would not gain access to data that it had no probable cause to collect. P.C. 3-4; see United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, J., concurring).

The State's basis for the sweeping and invasive search of electronic media ultimately rests on the detective's generic and vague assertions that "a suspect *may* try to conceal criminal evidence" and that "[c]riminals *can* mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade information." P.C. 12. The detective's broadly stated assertions are nothing more than an unfounded pronouncement that criminal suspects may be adept data hidiers. These

generic claims represent typical boiler plate language found in warrant applications, which have been picked up and presumed to be true by other courts. See e.g., United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006); United States v. Hunter, 13 F.Supp. 2d 574, 583 (D. Vt. 1998). However, one legal scholar tracked these presumed truths as they appeared in various court decisions and found that they ultimately returned to a Florida court case and were based on what one agent had been told by a Customs Service forensic computer expert. Paul Ohm, The Myth of the Superuser: Fear, Risk, and Harm Online, 41 U.C. Davis L Rev. 1327, 1355 (2008) (citing United States v. Abbell, 963 F. Supp. 1178, 1199 (S.D. Fla 1997)). No empirical data supports the suggestion that criminals generally have a greater propensity to be sophisticated data hidiers. Id. at 1342-1343. The factual record here shows someone who was hardly sophisticated about hiding evidence of his or her crime. Without any evidence that the suspect in this case possessed any exceptional computer prowess more than the ordinary user or that he or she used sophisticated programs or otherwise possessed knowledge of how to hide criminal evidence, the generic and vague statements in the affidavit fail to support the stringent probable cause requirements implicated by the facts of this case. The court was well within its discretion to so limit the scope of the search based on this evidence.

V. THE COURT WAS CORRECT AS A MATTER OF LAW THAT THE PLAIN VIEW DOCTRINE DOES NOT APPLY HERE AS THE NECESSARY CONDITIONS ARE NOT TRIGGERED AND IT WOULD HAVE TRANSFORMED THE WARRANT INTO A GENERAL AND OVERBROAD SEARCH

The starting point for the plain view doctrine is that it is an exception to the warrant requirement. As with all warrantless searches, these exceptions “must be jealously and carefully drawn” and “must be factually and narrowly tied to exigent

circumstances and reasonable expectations of privacy.” Savva, 159 Vt. at 85, 86, 616 A.2d at 779, 781 (quotations omitted). Police may lawfully seize evidence of a crime without a warrant if three conditions are satisfied: 1.) the officer was lawfully in a position from which to view the object seized; 2.) the object was in plain view and the incriminating nature of the object viewed was immediately apparent; and 3.) the officer must have lawful access to the object. Horton v. California, 496 U.S. 128, 136-137 (1990); Arizona v. Hicks, 480 U.S. 321, 326 (1987); State v. Trudeau, 165 Vt. 355, 358, 683 A.2d 725, 727 (1996). This last condition “is simply a corollary of the familiar principle discussed above, that no amount of probable cause can justify a warrantless search or seizure absent ‘exigent circumstances.’” Horton, 496 U.S. at 137, n.7 (quotations omitted); Trudeau, 165 Vt. at 361, 683 A.2d at 729. Only seizure of the object is permissible under the plain view doctrine; searches, however minimal, are not. Hicks, 480 U.S. at 325 (moving a stereo to view the serial number underneath was held to be an impermissible search even though the stereo was in plain view). “[T]aking action, unrelated to the objectives of the authorized intrusion, which exposed to view concealed portions of the apartment or its contents, [] produce[s] a new invasion of respondent’s privacy unjustified by the exigent circumstance that validated the entry. This is why...the distinction between looking at a suspicious object in plain view and moving it even a few inches is much more than trivial for purposes of the Fourth Amendment.” Id.

Because there is no plain viewing of data stored on electronic media and because there were no exigent circumstances as the police were in possession of the computer and there was no time limit to conduct the off-site search, the judge was correct that the plain view doctrine did not apply here. P.C. 3. Except for what appears on the screen when the

device is turned on, the data contained therein is entirely hidden from plain sight. To view the contents of data files, the forensic investigator must engage in separate acts to make that data plainly viewable, looking into file directories and sub-directories to locate the material sought. Susan W. Brenner and Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, 8 Mich. Telecomm. & Tech. L. Rev. 39, 94-95 (2002).

In the case of deleted, encrypted, or password protected files, the search requires added layers of complexity before the content of these files become discernible. While some deleted material may be viewed by opening up the trash or recycle directory, others require special software or processes to recover and view. Id. at 96. Each of these steps is a separate search, removing it even farther from the plain view doctrine. Walter, 447 U.S. at 653 (holding that search of film canisters—containers with labels plainly indicating that the contents contained obscene materials—was not justified and did not fall within the plain view doctrine as the film had to be removed and viewed on a projector); In re C.C., 2009 VT 108, ¶ 11, 186 Vt. 474, 480, 987 A.2d 1000, 1003 (rejecting the “plain feel” doctrine as the officer must be able to perceive the evidentiary nature of the object before its seizure).

Electronic data is essentially stored within several layers of closed containers located within the electronic device. See United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999). It is well-settled that under Article 11, the police cannot search a closed container without first obtaining a warrant. See e.g., Neil, 2008 VT 79, ¶ 10, 184 Vt. at 248, 958 A.2d at 1177-78. The State’s argument rests upon the presumption that the electronic device is the only container at issue. P.C. 21-22. This is essentially a version of

the “unworthy container” doctrine, an analysis that turns on the distinction of whether some containers are “worthy” of constitutional protection and others “unworthy.” Sayva, 159 Vt. at 89-90, 616 A.2d at 782. This doctrine has been flatly rejected by the Court. Id.

The principle behind the plain view doctrine is that Article 11 protections “do not attach to activities or possessions that ‘a person knowingly exposes to the public.’” State v. Rogers, 161 Vt. 236, 244, 638 A.2d 569, 573-574 (1993) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)). As in State v. Morris where the question concerned opaque trash bags, the issue here is not whether the police must avert their eyes to electronic data exposed to public viewing, but rather whether the police can sift through all electronic data stored on electronic devices, the contents of which are concealed from the public eye. 165 Vt. 111, 125, 680 A.2d 90, 100 (1996). Because the Court has recognized a “separate and higher” expectation of privacy for possessions located within the home not exposed to plain view and because the necessary prerequisites to the plain view doctrine are not met here, the judge was well within his discretion to so limit its use.

VI. THE STATE’S FACTUAL CLAIMS OF ADMINISTRATIVE INEFFICIENCIES HAVE NOT BEEN PREVIOUSLY FOUND BY THE JUDGE AND CANNOT BE RESOLVED BY THIS COURT, NOR DO THEY DIMINISH THE PROTECTIONS PROVIDED UNDER ARTICLE 11 AND V.R.Cr.P. 41

The State makes numerous factual claims in its brief about the negative impact that these conditions will have on criminal investigations: that the procedures outlined in the warrant are inconvenient and will “impede law enforcement[.]” State’s brief at 26-28. However, no court has made these findings and it is subject to serious dispute. See e.g., Brenner and Frederiksen, *supra* at 70-73;

For instance, the State's assertion that it must be able to open every data file contained in electronic media because it cannot otherwise know its contents is incorrect. State's brief at 26; P.C. 12. Though that notion may have been true in the past, advancements in digital forensics have provided technicians with powerful search and filter tools that can accurately identify relevant files and documents without subjecting the entirety of the computer to police scrutiny. Brenner and Frederiksen supra at 60, 95-96. See also "FTK Datasheet" http://accessdata.com/downloads/media/FTK_DataSheet.pdf (describing search capabilities of Forensic Toolkit software). In fact, expert forensic technicians place greater confidence in the capabilities of forensic software to identify relevant evidence than in a manual, file-by-file examination. See generally Ankid Agarwal, Megha Gupta, Saurabh Gupta, and Subhash Gupta "Systematic Digital Forensic Investigation Model" 5 Int. Journal of Computer Sci. and Sec. 118 (2011); Bob Carlson "Speeding the Digital Forensics Process: Bringing High Performance Computing Power into the Field" 7 Forensic Magazine 21-23 (2010). Such forensic software is commonplace at forensic laboratories and is not prohibitively expensive or difficult to obtain. In addition to the most popular commercial packages including Forensic Toolkit and EnCase, powerful forensic software, capable of advanced search and analysis, is available for free as open-source software. See Dan Manson et al. "Is the Open Way a Better Way? Digital Forensics using Open Source Tools" Proceedings of the 40th Annual Hawaii International Conference on System Sciences (2007).

Whether or not there are sufficient technological capabilities to implement the conditions imposed by the judge is a question that can only be answered by evidence and a hearing, not by appellate fact-finding. State v. Oney, 2009 VT 116, ¶ 13. n.6, -- Vt. --,

989 A.2d 995, 999 n.6. Even if the Court were to presume the facts asserted by the State to be true, the Court has repeatedly held that the protections of Article 11 do not diminish when police efficiency is at stake. State v. Morris, 165 Vt. 111, 126, 680 A.2d 90, 100 (1996); Bauder, 2007 VT 16, ¶ 37, 181 Vt. at 409, 924 A.2d at 52. Inconvenience to investigating police officers is “a slight price to pay for the fundamental rights preserved” by the Vermont Constitution. State v. Connolly, 133 Vt. 565, 570, 350 A.2d 364, 368 (1975). Changing technologies do not change this calculus. Bryant, 2008 VT 39, ¶ 29, 183 Vt. at 372, 950 A.2d at 479.

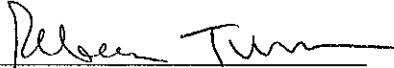
Speculation that the conditions severely impair law enforcement’s ability to do an effective search fails to meet the high burden in a petition for extraordinary relief to show that the judge usurped its authority. Forte, 154 Vt. at 48, 572 A.2d at 942.

CONCLUSION

For the reasons asserted above, the Office of the Defender General requests this Honorable Court to deny the State’s petition for extraordinary relief and affirm the court’s conditions imposed on the warrant. The Court should remand the matter to the lower court to correct and clarify that the conditions apply to all electronic media identified in the warrant and are not limited to devices belonging to Mr. Eric Gulfield.

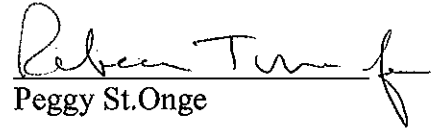
Dated on June 17, 2011 in Montpelier, Vermont.

Respectfully submitted,


Rebecca Turner, Esq.

CERTIFICATE OF COMPLIANCE

I certify that the above brief submitted under Rule 32(a)(7)(B) was typed using Microsoft Office Word 2003 and the word count is 8,882.


Peggy St. Onge