

IN THE SUPREME COURT OF THE STATE OF VERMONT

IN RE APPEAL OF APPLICATION FOR SEARCH WARRANT

Supreme Court Docket No. 2010-479

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

PETITIONER'S REPLY BRIEF

Attorneys for Petitioner State of Vermont:

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

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

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

On the brief:

William H. Sorrell, Esq.
Attorney General

Evan P. Meenan, Esq.
Assistant Attorney General

David E. Tartter, Esq.
Assistant Attorney General

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

ARGUMENT1

I. THE SPECIFIC CONDITIONS IMPOSED HERE ARE NOT PART OF EITHER THE PROBABLE CAUSE DETERMINATION OR THE REQUIREMENT OF PARTICULARITY.....1

II. THE NATURE OF ELECTRONIC STORAGE DOES NOT JUSTIFY A NEW FRAMEWORK ALLOWING THE JUDICIAL OFFICER TO DICTATE HOW THE SEARCH OF SUCH STORAGE MUST BE CONDUCTED.....3

III. THE OTHER LEGAL AUTHORITIES RELIED ON BY AMICI DO NOT SUPPORT THE IMPOSITION OF THE EX ANTE CONDITIONS HERE.5

 A. Article 11 Does Not Require Greater Restrictions In This Context Than The Fourth Amendment And Thus Does Not Provide Authority To Impose The Ex Ante Conditions.5

 B. The Main Federal Cases Relied Upon By Amici Do Not Support The Imposition Of The Ex Ante Conditions.....6

 C. Amici’s Other Examples Of Ex Ante Conditions Do Not Support Imposition Of The Conditions Here.....9

IV. NO JUDICIAL FACTFINDING IS NECESSARY TO ESTABLISH THAT THE CONDITIONS IMPOSED HERE MAY RESULT IN RELEVANT EVIDENCE NOT BEING FOUND.11

CONCLUSION.....12

CERTIFICATE OF COMPLIANCE.....13

TABLE OF AUTHORITIES

Cases

<i>Boyd v. United States</i> , 116 U.S. 616 (1886)	4
<i>Com. v. Scalise</i> , 439 N.E.2d 818 (Mass. 1982)	10, 11
<i>DeMassa v. Nunez</i> , 747 F.2d 1283 (9th Cir. 1984).....	10
<i>Deukmejian v. Superior Court</i> , 162 Cal.Rptr. 857 (Cal. Ct. App. 1980).....	9
<i>Frank v. State of Md.</i> , 359 U.S. 360 (1959).....	4
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	7
<i>In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621</i> , 321 F.Supp.2d 953 (N.D.Ill. 2004).....	8
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987).....	7
<i>Richards v. Wisconsin</i> , 520 U.S. 385 (1997)	10, 11
<i>State v. Arce</i> , 730 P.2d 1260 (Or. Ct. App. 1986)	10
<i>State v. Birchard</i> , 2010 VT 57, ___ Vt. ___, 5 A.3d 879	6
<i>State v. Meyer</i> , 167 Vt. 608, 708 A.2d 1343 (1998).....	6
<i>State v. Morris</i> , 165 Vt. 111, 680 A.2d 90 (1996).....	5, 6
<i>State v. Platt</i> , 154 Vt. 179, 574 A.2d 789 (1990)	6
<i>State v. Savva</i> , 159 Vt. 75, 616 A.2d 774 (1991).....	6
<i>State v. Sprague</i> , 2003 VT 20, 175 Vt. 123, 824 A.2d 539	6
<i>United States v. Banks</i> , 540 U.S. 31 (2003).....	10
<i>United States v. Brooks</i> , 427 F.3d 1246 (10th Cir. 2005).....	8
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999)	7, 8
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 579 F.3d 989 (9th Cir. 2009).....	6, 7
<i>United States v. Giberson</i> , 527 F.3d 882 (9th Cir. 2008)	4
<i>United States v. Hunter</i> , 13 F.Supp.2d 574 (D.Vt. 1998).....	4, 8, 9
<i>United States v. Ricciardelli</i> , 998 F.2d 8 (1st Cir. 1993).....	10
<i>United States v. Rowland</i> , 145 F.3d 1194 (10th Cir. 1998).....	10
<i>United States v. Williams</i> , 592 F.3d 511 (4th Cir. 2010), cert denied, 131 S.Ct. 595 (2010)	7
<i>Williams v. Broadbuss</i> , 331 Fed.Appx. 560, 2009 WL 1395463 (10th Cir. 2009).....	10

Rules

F.R.Cr.P. 41	9
V.R.Cr.P. 41.....	9

Constitutional Provisions

U.S. Const. amend. iv	passim
Vt. Const. art. 11	passim

Other Authorities

United States Dept. of Justice, United States Attorney's Manual § 9-13.420, 1999 WL 33219862 (2011).....	9
---	---

ARGUMENT

Amici make two main claims: (1) the judicial officer did not depart from established search warrant jurisprudence in imposing the ex ante conditions; and (2) searches of electronic devices are unique and thus require privacy protections beyond those imposed in searches of other property. Not only are these claims contradictory, they are also flawed.

I. THE SPECIFIC CONDITIONS IMPOSED HERE ARE NOT PART OF EITHER THE PROBABLE CAUSE DETERMINATION OR THE REQUIREMENT OF PARTICULARITY.

Amici agree that, in reviewing a search warrant, the judicial officer's main tool to protect privacy rights and prohibit general searches—whether the search is of a home, a vehicle, an office, or a computer—is the officer's review of probable cause and particularity. But while amici insist that the imposition of the ex ante conditions here is not a departure from this established process, they fail to explain how any of the specific conditions relate to particularity or probable cause. Indeed, they cannot, as these conditions dictate how the search must be conducted—for instance, specifying who will conduct it and which protocols will be used—not where, for what, and on what basis.

The Defender General's primary argument is that the affidavit as written does not provide probable cause for the breadth of the search sought and is not sufficiently particular. *See* Brief of the Defender General, Sections III, IV. This argument, however, does nothing to justify the particular ex ante conditions imposed here, as it offers no explanation as to how the specific conditions either serve to address the warrant's alleged deficiencies or are part of the judicial officer's authority to ensure probable cause and

particularity.¹ Moreover, as with search warrants in every other context, this argument is properly raised through a motion to suppress and the resulting ex post review, rather than in a petition for extraordinary relief involving a different issue.²

The ACLU similarly fails to address how any of the specific conditions imposed here are justified under the judicial officer's authority to ensure probable cause and particularity, arguing only that each of the conditions "is a reasonable measure to protect privacy." Brief of the ACLU, Section III.C. But the issue is not whether the conditions imposed here limit the privacy invasion. There could be innumerable conditions imposed in this and every search that do that, but a judicial officer is not free to impose whatever conditions he wishes, free from the constitutional and statutory bounds of his authority. The issue, rather, is whether the judicial officer acted within this authority when he imposed the specific conditions imposed here. The answer is that he did not.

The ex ante conditions, in fact, fail to protect privacy interests at all. For instance, the abrogation of the plain view doctrine does not prevent private documents from being viewed, but only prevents them from being used in a criminal prosecution. Similarly, the firewall between investigator and forensic examiner does not prevent the privacy

¹ The Defender General directly addresses only one of the ex ante conditions, arguing that plain view does not apply in this context because "[e]lectronic data is essentially stored within several layers of closed containers located within the electronic device," and law enforcement needs a separate warrant to open each of those "closed containers." Brief of the Defender General, Section V. Under this argument, however, if law enforcement obtained a warrant to search a file cabinet for documents of tax fraud, for example, it could only pull the files from the file cabinet but could not search them without obtaining a separate warrant for each file. This makes no sense, constitutionally or practically.

² The claim that the warrant as written was insufficiently particular should not be addressed in this appeal, because (1) the claim that the State raises in its petition for extraordinary relief concerns only the imposition of the ex ante conditions, and (2) concerns about the particularity of the warrant as written are properly addressed ex post, through a motion to suppress, as is done with all other warrants. However, should the Court decide to address this issue and find that the warrant as written failed for particularity, it should remand the matter to the judicial officer for further proceedings.

intrusion, as the search may be intrusive regardless of who conducts it. And, as stated in the State's principal brief, the forensic examiner is as likely or unlikely as the investigator to expand the search of the computer beyond the limits of the warrant. In short, the ex ante conditions are not justified either by any alleged privacy protections they provide or by the judicial officer's authority to ensure particularity and probable cause.

II. THE NATURE OF ELECTRONIC STORAGE DOES NOT JUSTIFY A NEW FRAMEWORK ALLOWING THE JUDICIAL OFFICER TO DICTATE HOW THE SEARCH OF SUCH STORAGE MUST BE CONDUCTED.

Amici's second main claim is that searches of electronic devices are unique and thus require increased privacy protections. For instance, both amici argue that principles that apply to the search of closed containers or file cabinets do not apply here. *See* Brief of the Defender General, at 26-27; Brief of the ACLU, Section I.B. The ACLU goes further, arguing that "[s]earches of electronic devices implicate heightened concerns of privacy and dignity that distinguish the devices from other types of property." Brief of the ACLU, at 7. The Defender General also argues that ex post review (applicable to all other types of searches) does not sufficiently protect the privacy rights of defendants and third parties in this context. *See* Brief of the Defender General, Section II. Yet both the Defender General and the ACLU fail to explain how there is any qualitative, constitutionally-based difference between the search of a computer and the search of a home or office or vehicle such that a different framework is necessary.³ As the Ninth Circuit has stated, heightened privacy protections for computer searches must be "based on a principle that is not technology-specific," as "neither the quantity of information, nor

³ The Defender General also fails to explain why civil remedies available in other search contexts to third parties whose privacy rights may have been violated do not suffice to protect third parties in the computer storage context.

the form in which it is stored, is legally relevant in the Fourth Amendment context.”

United States v. Giberson, 527 F.3d 882, 887-88 (9th Cir. 2008).

The Defender General, and to some extent the ACLU, also argue that any search of an entire computer is so invasive that it is “the modern day equivalent of the general warrant.” Brief of the Defender General, Section III.C; *see also* Brief of the ACLU, at 10 (“This rationale would lead to an unreasonable result: every computer file in every computer will always be searchable in the off chance it may contain evidence. There would be no limits to these types of searches. The State’s rationale would therefore have Vermont judges routinely issue general warrants, the precise thing the Fourth Amendment was enacted to prevent.”). This claim is incorrect. The Fourth Amendment and Article 11 were designed in part to prevent general warrants—so-called “because they authorized searches in any place, for any thing,” *Boyd v. United States*, 116 U.S. 616, 641 (1886) (Miller, J., concurring)—not to prevent invasive searches altogether. *See, e.g., Frank v. State of Md.*, 359 U.S. 360, 381-82 (1959) (Douglas, J., dissenting) (the Fourth Amendment “was designed to protect the citizen against uncontrolled invasion of his privacy. It does not make the home a place of refuge from the law. It only requires the sanction of the judiciary rather than the executive before that privacy may be invaded.”). Simply because a warrant authorizes law enforcement to conduct an invasive search of a computer does not lead to the conclusion that it is automatically a “general warrant.” *See, e.g., United States v. Hunter*, 13 F.Supp.2d 574, 584 (D.Vt. 1998) (“[C]omputer searches are not per se overbroad ...”).

In fact, even if a computer does contain numerous intermingled documents, files, etc., a search of the entirety of that computer is not necessarily any more intrusive, or

more greatly implicates privacy concerns, than the search of the entirety of a house. In searching a house for drugs, a murder weapon, or forged checks pursuant to the appropriate warrant, the officers will be able to look everywhere in the house, including in the bedroom, in dressers and closets; in the bathroom, in medicine chests; in the kitchen, in the cabinets and the refrigerator; in the study, in desks and file cabinets; and in every room's trash, which contains "intimate details of people's lives." *State v. Morris*, 165 Vt. 111, 117, 680 A.2d 90, 94 (1996) . In sum, there is no principled, constitutional basis for departing from existing search warrant procedure when the search involves a computer rather than a house or car or office.

III. THE OTHER LEGAL AUTHORITIES RELIED ON BY AMICI DO NOT SUPPORT THE IMPOSITION OF THE EX ANTE CONDITIONS HERE.

Amici also rely on other legal authorities—Article 11, federal caselaw, and alleged examples of the use of ex ante conditions in other contexts—to argue that the imposition of the ex ante conditions here was proper. None of these authorities, however, provide support for the judicial officer's actions in this case.

A. Article 11 Does Not Require Greater Restrictions In This Context Than The Fourth Amendment And Thus Does Not Provide Authority To Impose The Ex Ante Conditions.

The Defender General claims that Article 11 provides the authority to impose the ex ante conditions because it imposes a "least intrusive" requirement for all searches, including those conducted pursuant to a warrant. *See* Brief of the Defender General, Section I.B. This Court, though, has never imposed such a requirement. Rather, this Court has used the "least intrusive" language primarily in the context of warrantless searches, requiring that "when acting without a warrant, police [must] operate 'in the least intrusive manner possible under the circumstances.'" *State v. Savva*, 159 Vt. 75, 88-

89, 616 A.2d 774, 781 (1991) (quoting *State v. Platt*, 154 Vt. 179, 188, 574 A.2d 789, 794 (1990)); see also *State v. Birchard*, 2010 VT 57, ¶ 5, ___ Vt. ___, 5 A.3d 879 (“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, obtaining a defendant’s permission to search or seeking the oversight of a magistrate.”). And while this Court has held that there are circumstances in which Article 11 requires a warrant but where the Fourth Amendment would not, see, e.g., *State v. Sprague*, 2003 VT 20, ¶¶ 13-20, 175 Vt. 123, 824 A.2d 539 (Article 11 requires particular justification for an exit order in automobile stops); *Morris*, 165 Vt. at 114, 680 A.2d at 93 (Article 11 requires a warrant to search a person’s trash placed in opaque bags at roadside), it has specifically declined to go beyond that and impose greater privacy protections when it comes to searches pursuant to a warrant. See, e.g., *State v. Meyer*, 167 Vt. 608, 708 A.2d 1343 (1998) (rejecting argument that Article 11 prohibited the search of a home pursuant to a valid search warrant if the homeowner is not present; holding that while “Article 11 has more specific requirements for warrants [than the Fourth Amendment], [it] does not mention the circumstances involved here”). In no context, whether the search involves a car, an office, a home, or any other place, has this Court suggested that, once the warrant is obtained, special procedures must be followed to further protect privacy interests.

B. The Main Federal Cases Relied Upon By Amici Do Not Support The Imposition Of The Ex Ante Conditions.

The ACLU argues that other federal courts have imposed similar ex ante limits on electronic searches, pointing to the *CDT* case and others. None of these cases, however, support the ACLU’s position.

With regard to *CDT*, the ACLU offers no response to the arguments that this case should not be relied upon because it has been superseded, is advisory only, has been rejected by numerous courts, and is factually dissimilar to the case at bar. Moreover, the ACLU argues that *CDT* “simply applies preexisting Fourth Amendment law to computer searches,” Brief of the ACLU, at 15, but like *CDT*, fails to offer any analysis as to how the specific conditions, such as the abrogation of the plain view doctrine, are supported by Fourth Amendment jurisprudence.

The other main federal cases relied on by the ACLU similarly do not support the imposition of the ex ante conditions here. For instance, in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), a police officer inadvertently came across a child pornography JPG file while searching a computer for evidence of drug sales, pursuant to a warrant. *Id.* at 1271. The officer then proceeded to examine JPG file after JPG file, searching for more child pornography rather than for the evidence sought by the warrant. *Id.* at 1271, 1273. The Tenth Circuit ruled that since all but the first photograph were not “inadvertently discovered,” the plain view doctrine did not apply to those subsequent photographs, which as such would be suppressed. *Id.* at 1273, 1273 n.4. This inadvertence requirement, however, has been soundly rejected. *See, e.g., United States v. Williams*, 592 F.3d 511, 523 (4th Cir. 2010), cert denied, 131 S.Ct. 595 (2010) (holding that an “inadvertence” requirement “cannot stand against the principle, well-established in Supreme Court jurisprudence, that the scope of a search conducted pursuant to a warrant is defined *objectively* by the terms of the warrant and the evidence sought, not by the *subjective* motivations of an officer.”) (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) and *Horton v. California*, 496 U.S. 128, 130, 138 (1990)). Moreover, *Carey*

actually supports the application of the plain view doctrine to computer searches, as the court specifically stated that its holding that the photographs not “inadvertently” found were not subject to the plain view exception, did not apply to the first photograph discovered, which in fact was discovered inadvertently. 592 F.3d at 1273 n.4.

Another case cited by the ACLU, *In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621*, 321 F.Supp.2d 953 (N.D.Ill. 2004), relied on *Carey* in holding that a warrant for the search of a computer must specify the search protocol to be used if it is to satisfy the particularity requirement of the Fourth Amendment. *Id.* at 960-61. The Tenth Circuit, however, has explicitly rejected this reading of *Carey*. See *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) (“This court has never required warrants to contain a particularized computer search strategy.”). Moreover, like amici here, the court in *3817 W. West End* fails to explain its conceptual jump from describing the particularity requirement to arguing that the government must “provide a better description of *how* it seeks to go about searching the computer.” 321 F.Supp.2d at 960 (emphasis added).

Finally, the case of *United States v. Hunter*, 13 F.Supp.2d 574 (D.Vt. 1998) cited by the ACLU fully supports the State’s position here. In *Hunter*, the government sought a warrant to search a lawyer’s office, including computers, and specified in the warrant a protocol it would use in the execution of the warrant to minimize the invasion of materials protected by the attorney-client privilege. *Id.* at 578. The court held that the warrant was not an impermissible general warrant, although it failed for particularity because it did not indicate the specific crimes for which the computers and computer records were sought. *Id.* at 582-85. In so holding, the *Hunter* court explicitly rejected the claim that all computer searches are general searches requiring a new paradigm and

instead embraced a case-by-case probable cause and particularity analysis. *Id.* at 584. This is exactly the approach used in all other warrant searches conducted in Vermont, exactly the approach advocated by the State here, and exactly the opposite of the approach taken by the judicial officer. And while the *Hunter* court pointed to the government's proposed reviewing plan as an example of how the government could ensure that the particularity requirement is not violated, *id.* at 584-85, at no point did the court indicate that such a protocol was required or that the court had the authority to impose such a requirement.

C. Amici's Other Examples Of Ex Ante Conditions Do Not Support Imposition Of The Conditions Here.

Amici further attempt to support the ex ante conditions here by pointing to other examples of ex ante regulation of warrants. *See* Brief of the Defender General, Section I.C; Brief of the ACLU, at 10-11. None of these examples, however, provide support for the judicial officer's actions in this case.

First, amici point to several provisions of V.R.Cr.P. 41 and F.R.Cr.P. 41, which allow the judicial officer to specify when the warrant must be executed and the return must be made. This is straightforward legislative authorization, which is absent here.

Amici also point to the use of special masters. However, special masters are generally authorized by statute, *see, e.g., Deukmejian v. Superior Court*, 162 Cal.Rptr. 857, 861 (Cal. Ct. App. 1980), or are part of guidelines for practice put in place by prosecutors, which do not provide any authority to judicial officers, *see, e.g., United States Dept. of Justice, United States Attorney's Manual § 9-13.420*, 1999 WL 33219862 (2011). Moreover, special masters are used in a specific context, namely, where the search implicates legal privileges, such as the attorney-client privilege. *See, e.g.,*

DeMassa v. Nunez, 747 F.2d 1283 (9th Cir. 1984) (attorney-client privilege); *Williams v. Broaddus*, 331 Fed.Appx. 560, 2009 WL 1395463 (10th Cir. 2009) (same).⁴ No such privilege is involved here.

The Defender General emphasizes the authority to issue anticipatory warrants, but that authority stems directly from the power to ensure that the search is supported by probable cause. *See, e.g., United States v. Ricciardelli*, 998 F.2d 8, 11 (1st Cir. 1993) (“In either instance, contemporary or anticipatory, the focal point of the magistrate’s inquiry is whether there is probable cause to think that the contraband will be at the place to be searched at the time of the contemplated intrusion.”); *United States v. Rowland*, 145 F.3d 1194, 1201 (10th Cir. 1998) (“In principle, the use of a ‘triggering event’ can help assure that the search takes place only when justified by ‘probable cause.’”) (citation omitted). The conditions imposed here, in contrast, have no relation to probable cause.

Finally, amici point to the practice of issuing no-knock warrants. The basis for the authority to issue no-knock warrants, however, is not clearly established. Compare *United States v. Banks*, 540 U.S. 31, 36 (2003) (no-knock warrants authorized under common law); *Com. v. Scalise*, 439 N.E.2d 818, 822 (Mass. 1982) (same) with *Richards v. Wisconsin*, 520 U.S. 385, 396 n.7 (1997) (citing state statutes authorizing no-knock warrants); *State v. Arce*, 730 P.2d 1260, 1261-62 (Or. Ct. App. 1986) (a judge has no authority to abrogate the knock-and-announce requirement absent an authorizing statute). More importantly, there is a significant difference between no-knock warrants and the ex ante conditions here. No-knock warrants take a clear constitutional principle—that the knock-and-announce rule need not be followed if there are exigent circumstances—and

⁴ The ACLU relies on both *DeMassa* and *Williams*, but neither case involved a challenge to the court’s authority to require the use of a special master, and thus neither analyzed the issue.

allow the judicial officer to apply it ahead of time, based on facts detailed in the application. In contrast, the conditions imposed here have no clear basis in Fourth Amendment or Article 11 jurisprudence, and indeed expand privacy rights beyond what those authorities require.

It is also worth noting that, whether a no-knock warrant is granted or explicitly denied, police are ultimately bound by the Fourth Amendment, not by the no-knock terms of the warrant. *See, e.g., Richards*, 520 U.S. at 395-96 (search was constitutional where police, despite judicial officer's explicit rejection of request for no-knock warrant, failed to knock prior to entering premises, given circumstance present at the time of the execution of the warrant); *Scalise*, 439 N.E.2d at 823 (if "the facts existing at the time the warrant is issued ... no longer exist at the time the warrant is executed ... the officers would be required to knock and announce their purpose"). Similarly, as argued in the State's main brief, the computer search should ultimately be analyzed *ex post* according to its constitutional reasonableness, not whether it conformed to the conditions, thus making those conditions in effect superfluous.

IV. NO JUDICIAL FACTFINDING IS NECESSARY TO ESTABLISH THAT THE CONDITIONS IMPOSED HERE MAY RESULT IN RELEVANT EVIDENCE NOT BEING FOUND.

The Defender General's final point of contention—that "[t]he State's factual claims of administrative inefficiencies" cannot be resolved without further fact-finding, *see* Brief of the Defender General, Section VI—misses the point of the State's argument. The State's claim here is not that the imposed conditions are "administrative inefficiencies" or "inconveniences." Rather, the claim is that conditions such as the abrogation of the plain view doctrine, the firewall between investigator and forensic examiner, and the pre-specification of search protocols, create the potential that existing

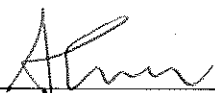
relevant evidence will be overlooked. For the purposes of this appeal, there is no need for factual development to determine if the State has the practical ability to comply with these conditions: even if the State can comply, this does not eliminate the possibility that relevant evidence could exist yet not be found.

Indeed, to the extent that factual development pertaining to possible “inconveniences” or “efficiencies” involved in compliance with the conditions is necessary, this shows that, regardless of the limits of the judicial officer’s authority, these conditions are more appropriately considered at the legislative level. There, such an analysis can be undertaken by the legislature as part of its examination into whether the nature of electronic storage necessitates the implementation of privacy protections beyond those provided by the Fourth Amendment and Article 11.

CONCLUSION

While the judiciary has constitutional and statutory authority to balance individual privacy interests against the public’s interest in effective law enforcement, the judicial officer here exceeded that authority and expanded privacy protections in a way that is more appropriately left to the legislature. Thus, for the reasons presented here and in its principal brief, the State requests that this Court strike the ex ante conditions imposed on the search warrant.

Dated at Burlington, Vermont on this 1 day of July, 2011.

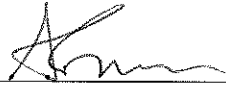


Andrew R. Strauss
Deputy State’s Attorney
Chittenden County State’s Attorneys Office

CERTIFICATE OF COMPLIANCE

The undersigned certifies that Petitioner's Reply Brief in Docket No. 2010-479 complies with the word-count limitation of V.R.A.P. 32(a)(7). The number of pertinent words in Petitioner's Brief is 3,755. Microsoft Word was used.

Dated at Burlington, Vermont on this 1 day of July, 2011.



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