Thanh Long Vu *Appellant*

v.

Her Majesty The Queen *Respondent*

and

Attorney General of Ontario, Attorney General of Alberta, British Columbia Civil Liberties Association, Canadian Civil Liberties Association and Criminal Lawyers' Association (Ontario) *Interveners*

Indexed as: R. *v.* Vu

2013 SCC 60

File No.: 34687.

2013: March 27; 2013: November 7.

Present: McLachlin C.J. and LeBel, Fish, Abella, Rothstein, Cromwell, Moldaver, Karakatsanis and Wagner JJ.

ON APPEAL FROM THE COURT OF APPEAL FOR BRITISH COLUMBIA

Constitutional law — Charter of Rights — Search and seizure — Validity of search — Police obtaining warrant not specifying grounds for obtaining evidence of ownership or occupancy of residence and not mentioning search of computers and cellular telephones — Whether search warrant properly permitting a search for documents evidencing ownership or occupation — Whether warrant authorized search of computers and cellular telephone — If search was unlawful, whether evidence obtained should be excluded — Canadian Charter of Rights and Freedoms, ss. 8, 24(2).

The appellant was charged with production of marijuana, possession of marijuana for the purpose of trafficking, and theft of electricity. The police had obtained a warrant authorizing the search of a residence for evidence of theft of electricity, including documentation identifying the owners and/or occupants of the residence. Even

Thanh Long Vu *Appelant*

c.

Sa Majesté la Reine *Intimée*

et

Procureur général de l'Ontario, procureur général de l'Alberta, Association des libertés civiles de la Colombie-Britannique, Association canadienne des libertés civiles et Criminal Lawyers' Association (Ontario) *Intervenants*

Répertorié : R. *c.* Vu

2013 CSC 60

N° du greffe : 34687.

2013 : 27 mars; 2013 : 7 novembre.

Présents : La juge en chef McLachlin et les juges LeBel, Fish, Abella, Rothstein, Cromwell, Moldaver, Karakatsanis et Wagner.

EN APPEL DE LA COUR D'APPEL DE LA COLOMBIE-BRITANNIQUE

Droit constitutionnel — Charte des droits — Fouilles, perquisitions et saisies — Validité de la fouille — Obtention par la police d'un mandat ne précisant pas les motifs de la recherche de preuves confirmant l'identité des propriétaires ou occupants d'une résidence et ne mentionnant pas la fouille d'ordinateurs et de téléphones cellulaires — Le mandat de perquisition autorisait-il dûment la recherche de documents confirmant l'identité des propriétaires ou occupants? — Le mandat autorisait-il la fouille des ordinateurs et du téléphone cellulaire? — Si la fouille était illégale, la preuve obtenue devait-elle être écartée? — Charte canadienne des droits et libertés, art. 8, 24(2).

L'appelant a été accusé de production de marijuana, de possession de marijuana en vue d'en faire le trafic et de vol d'électricité. Les policiers ont obtenu un mandat les autorisant à perquisitionner dans une résidence pour y rechercher des preuves de vol d'électricité, y compris des documents identifiant les propriétaires et/ou occupants

though the Information to Obtain ("ITO") indicated that the police intended to search for "computer generated notes", the warrant did not specifically refer to computers or authorize the search of computers. In the course of their search of the residence, police found marijuana, two computers and a cellular telephone. A search of the devices revealed evidence that the appellant was the occupant. At trial, he claimed that the searches had violated his s. 8 *Charter* rights. The trial judge concluded that the ITO did not establish reasonable grounds to believe that documents identifying the owners and/or occupants would be found in the residence and so the warrant could not authorize the search for them. Further, the police were not authorized to search the personal computers and cellular telephone because those devices were not specifically mentioned in the warrant. She excluded most of the evidence found as a result of these searches and acquitted the appellant of the drug charges. The Court of Appeal set aside the acquittals and ordered a new trial on the grounds that the warrant had properly authorized the searches and that there had been no breach of the appellant's s. 8 *Charter* rights.

Held: The appeal should be dismissed.

The traditional legal framework holds that once police obtain a warrant to search a place for certain things, they do not require specific, prior authorization to search in receptacles such as cupboards and filing cabinets. The question in this case is whether this framework is appropriate for computer searches. Computers differ in important ways from the receptacles governed by the traditional framework and computer searches give rise to particular privacy concerns that are not sufficiently addressed by that approach.

The first issue that arises in this case is whether the search warrant properly permitted a search for documents identifying the owners and/or occupants. Although the trial judge found that the ITO did not contain a statement by its author that there were reasonable grounds to believe that such documents would be found in the residence, the ITO set out facts sufficient to allow the authorizing justice to reasonably draw that inference. The search for such

de la résidence. Même si la Dénonciation en vue d'obtenir un mandat de perquisition (« Dénonciation ») indiquait que les policiers entendaient chercher « des notes générées par ordinateur », le mandat ne faisait pas expressément mention des ordinateurs et n'autorisait pas non plus la fouille de tels appareils. Durant la perquisition dans la résidence, les policiers ont trouvé de la marijuana, deux ordinateurs et un téléphone cellulaire. La fouille de ces appareils a permis de découvrir des éléments de preuve établissant que l'appelant était l'occupant de la résidence. Au procès, l'appelant a soutenu que les fouilles avaient violé les droits que lui garantit l'art. 8 de la *Charte*. La juge de première instance a conclu que la Dénonciation ne démontrait pas l'existence de motifs raisonnables de croire que des documents confirmant l'identité des propriétaires et/ou occupants seraient trouvés dans la résidence, et qu'en conséquence le mandat ne pouvait autoriser leur recherche. En outre, les policiers n'étaient pas autorisés à fouiller les ordinateurs personnels et le téléphone cellulaire, parce que ces appareils n'étaient pas expressément mentionnés dans le mandat. La juge de première instance a écarté la plupart des éléments de preuve découverts par suite de ces fouilles, et elle a acquitté l'appelant des accusations liées à la drogue. La Cour d'appel a annulé les acquittements et ordonné la tenue d'un nouveau procès, au motif que le mandat avait dûment autorisé les fouilles et qu'il n'y avait eu aucune violation des droits garantis à l'appelant par l'art. 8 de la *Charte*.

Arrêt : Le pourvoi est rejeté.

Selon le cadre juridique traditionnel, lorsque des policiers obtiennent un mandat les autorisant à perquisitionner dans un lieu et à y chercher certaines choses, ils n'ont pas besoin d'obtenir une autorisation expresse préalable pour fouiller dans des contenants tels que des placards et des classeurs. Il s'agit en l'espèce de déterminer si ce cadre juridique convient à la fouille des ordinateurs. Les ordinateurs diffèrent à bien des égards des contenants visés par le cadre juridique traditionnel, et la fouille des ordinateurs soulève, en matière de respect de la vie privée, des préoccupations particulières dont ne tient pas suffisamment compte cette approche.

La première question soulevée en l'espèce consiste à déterminer si le mandat de perquisition autorisait dûment la recherche de documents identifiant les propriétaires et/ou occupants. Bien que la juge de première instance ait conclu que la Dénonciation ne contenait aucune déclaration de son auteur indiquant qu'il existait des motifs raisonnables de croire que de tels documents seraient découverts dans la résidence, la Dénonciation énonçait

material, therefore, did not breach the appellant's rights under s. 8 of the *Charter*.

The second issue is whether the warrant authorized the search of the computers and cellular telephone. Section 8 of the *Charter* — which gives everyone the right to be free of unreasonable searches and seizures — seeks to strike an appropriate balance between the right to be free of state interference and the legitimate needs of law enforcement. This balance is generally achieved in two main ways. First, the police must obtain judicial authorization for a search *before* they conduct it, usually in the form of a search warrant. Second, an authorized search must be conducted in a reasonable manner, ensuring that the search is no more intrusive than is reasonably necessary to achieve its objectives. The privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets. It is difficult to imagine a more intrusive invasion of privacy than the search of a personal or home computer. Computers potentially give police access to an almost unlimited universe of information that users cannot control, that they may not even be aware of, may have tried to erase and which may not be, in any meaningful sense, located in the place of search. The numerous and striking differences between computers and traditional receptacles call for distinctive treatment under s. 8 of the *Charter*. The animating assumption of the traditional rule — that if the search of a place is justified, so is the search of receptacles found within it — simply cannot apply with respect to computer searches.

In effect, the privacy interests at stake when computers are searched require that those devices be treated, to a certain extent, as a separate place. Prior authorization of searches is a cornerstone of our search and seizure law. The purpose of the prior authorization process is to balance the privacy interest of the individual against the interest of the state in investigating criminal activity *before* the state intrusion occurs. Only a specific, prior authorization to search a computer found in the place

suffisamment de faits pour permettre au juge de paix saisi de la demande d'autorisation de tirer raisonnablement cette inférence. Les fouilles visant de tels documents n'ont donc pas violé les droits garantis à l'appelant par l'art. 8 de la *Charte*.

La deuxième question est de savoir si le mandat autorisait la fouille des ordinateurs et du téléphone cellulaire. L'article 8 de la *Charte* — qui confère à chacun le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives — vise à établir un juste équilibre entre le droit à la protection contre l'ingérence de l'État et la nécessité légitime de faire respecter la loi. Cet équilibre est généralement réalisé grâce à deux moyens principaux. Premièrement, les policiers doivent obtenir des tribunaux l'autorisation d'effectuer une perquisition *avant* de procéder à celle-ci, autorisation qui prend habituellement la forme d'un mandat de perquisition. Deuxièmement, la perquisition ainsi autorisée doit être effectuée d'une manière non abusive, ce qui permet d'éviter que la perquisition ait un caractère plus envahissant que ce qui est raisonnablement nécessaire pour atteindre ses objectifs. Les intérêts en matière de respect de la vie privée que met en jeu la fouille des ordinateurs diffèrent nettement de ceux en cause lors de la fouille de contenants tels des placards et des classeurs. Il est difficile d'imaginer une atteinte plus grave à la vie privée d'une personne que la fouille de son ordinateur personnel. Les ordinateurs sont susceptibles de donner aux policiers accès à un univers presque illimité d'informations sur lesquelles les utilisateurs n'ont aucune maîtrise, dont ils ne connaissent peut-être même pas l'existence, qu'ils peuvent avoir tenté d'effacer, et qui d'ailleurs pourraient fort bien ne pas se trouver concrètement dans le lieu fouillé. Les différences nombreuses et frappantes entre les ordinateurs et les contenants traditionnels commandent que ces objets soient traités différemment pour l'application de l'art. 8 de la *Charte*. L'hypothèse fondamentale à la base de la règle traditionnelle — à savoir que si la perquisition effectuée dans un lieu est justifiée, la fouille des contenants découverts dans ce lieu l'est également — ne peut tout simplement pas s'appliquer à la fouille des ordinateurs.

En effet, en raison des intérêts en matière de vie privée que soulève la fouille d'un ordinateur, un tel appareil doit, dans une certaine mesure, être traité comme un lieu distinct. L'autorisation préalable des perquisitions constitue une assise fondamentale de notre droit relatif aux fouilles, perquisitions et saisies. L'objectif du processus d'autorisation préalable est de mettre en balance le droit à la vie privée du particulier et l'intérêt de l'État à enquêter sur une activité criminelle, *avant*

of search ensures that the authorizing justice has considered the full range of the distinctive privacy concerns raised by computer searches and, having done so, has decided that this threshold has been reached in the circumstances of a particular proposed search. This means that if police intend to search any computers found within a place they want to search, they must first satisfy the authorizing justice that they have reasonable grounds to believe that any computers they discover will contain the things they are looking for. If police come across a computer in the course of a search and their warrant does not provide specific authorization to search computers, they may seize the computer, and do what is necessary to ensure the integrity of the data. If they wish to search the data, however, they must obtain a separate warrant. In this case, the authorizing justice was not required to impose a search protocol in advance with conditions limiting the manner of the search. While such conditions may be appropriate in some cases, they are not, as a general rule, constitutionally required.

Having found that the search here was unlawful, the final issue is whether the evidence obtained should be excluded. Section 24(2) of the *Charter* requires that evidence obtained in a manner that infringes the rights of an accused under the *Charter* be excluded from the trial if it is established that "having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute". Here, the ITO did refer to the intention of the officers to search for computer-generated documents and considering that the state of the law with respect to computer searches was uncertain when police carried out their investigation and the otherwise reasonable manner in which the search was conducted, the violation was not serious. Further, there was a clear societal interest in adjudicating on their merits charges of production and possession of marijuana for the purpose of trafficking. Balancing these factors, the evidence should not be excluded. The police believed on reasonable grounds that the search of the computer was authorized by the warrant. While every search of a personal or home computer is a significant invasion of privacy, the search here did not step outside the purposes for which the warrant had been issued.

que l'intrusion de l'État ne se produise. Seule une autorisation expresse préalable de fouiller des ordinateurs susceptibles d'être découverts dans le lieu perquisitionné garantit que le juge de paix qui a statué sur la demande d'autorisation a pris en compte l'ensemble des préoccupations distinctives en matière de vie privée que soulève la fouille de ces appareils, puis déterminé que ce critère était respecté eu égard aux circonstances de la fouille particulière projetée. Cela signifie que, si des policiers entendent fouiller tout ordinateur trouvé dans le lieu qu'ils souhaitent perquisitionner, ils doivent d'abord convaincre le juge de paix saisi de la demande d'autorisation qu'ils possèdent des motifs raisonnables de croire que les ordinateurs qu'ils pourraient découvrir contiendront les choses qu'ils recherchent. Si, durant une perquisition, les policiers trouvent un ordinateur et que leur mandat ne les autorise pas expressément à fouiller les ordinateurs, ils peuvent le saisir et prendre les mesures nécessaires pour assurer l'intégrité des données. Toutefois, s'ils désirent consulter ces données, ils doivent obtenir un mandat distinct. En l'espèce, le juge de paix saisi de la demande d'autorisation n'était pas tenu d'imposer à l'avance un protocole de perquisition assorti de conditions limitant la façon de procéder à la fouille. Quoique de telles conditions puissent convenir dans certains cas, elles ne sont pas, en règle générale, requises par la Constitution.

Comme il a été conclu que la fouille effectuée dans la présente affaire était illégale, la dernière question qui se pose est de savoir si la preuve obtenue devrait être écartée. Le paragraphe 24(2) de la *Charte* exige que les éléments de preuve obtenus d'une manière qui porte atteinte aux droits garantis à l'accusé par la *Charte* soient écartés du procès s'il est établi, « eu égard aux circonstances, que leur utilisation est susceptible de déconsidérer l'administration de la justice ». En l'espèce, la Dénonciation faisait effectivement mention de l'intention des policiers de rechercher des documents générés par ordinateur et, vu l'état incertain du droit applicable à la fouille d'ordinateurs au moment où les policiers ont effectué leur enquête et la manière par ailleurs non abusive dont la fouille a été effectuée, la violation n'était pas grave. En outre, il était manifestement dans l'intérêt de la société que des accusations de production et de possession de marijuana en vue d'en faire le trafic soient jugées au fond. Il ressort de la mise en balance de ces différents facteurs que les éléments de preuve ne doivent pas être écartés. Les policiers possédaient des motifs raisonnables de croire que la fouille de l'ordinateur était autorisée par le mandat. Bien que toute fouille d'un ordinateur personnel constitue une atteinte importante à la vie privée, la fouille effectuée en l'espèce n'a pas débordé les objectifs pour lesquels le mandat avait été décerné.

Cases Cited

Applied: *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145; *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353; **referred to:** *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992; *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253; *R. v. Shiers*, 2003 NSCA 138, 219 N.S.R. (2d) 196; *R. v. Sanchez* (1994), 93 C.C.C. (3d) 357; *R. v. Allain* (1998), 205 N.B.R. (2d) 201; *R. v. E. Star International Inc.*, 2009 ONCJ 576 (CanLII); *BGI Atlantic Inc. v. Canada (Minister of Fisheries and Oceans)*, 2004 NLSCTD 165, 241 Nfld. & P.E.I.R. 206; *R. v. Charles*, 2012 ONSC 2001, 258 C.R.R. (2d) 33; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Mohamad* (2004), 69 O.R. (3d) 481; *R. v. Boudreau-Fontaine*, 2010 QCCA 1108 (CanLII); *Descôteaux v. Mierzwinski*, [1982] 1 S.C.R. 860; *Lavallee, Rackel & Heintz v. Canada (Attorney General)*, 2002 SCC 61, [2002] 3 S.C.R. 209; *United States v. Carey*, 172 F.3d 1268 (1999); *United States v. Burgess*, 576 F.3d 1078 (2009); *United States v. Christie*, 717 F.3d 1156 (2013); *R. v. Côté*, 2011 SCC 46, [2011] 3 S.C.R. 215.

Statutes and Regulations Cited

Canadian Charter of Rights and Freedoms, ss. 8, 24(2).
Criminal Code, R.S.C. 1985, c. C-46, ss. 186(4)(*d*), 326(1)(*a*), 487, 487.1, 488, 488.1.
Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Authors Cited

Fontana, James A., and David Keeshan. *The Law of Search and Seizure in Canada*, 8th ed. Markham, Ont.: LexisNexis, 2010.
Gold, Alan D. "Applying Section 8 in the Digital World: Seizures and Searches". Paper prepared for the Law Society of Upper Canada, 7th Annual Six-Minute Criminal Defence Lawyer, June 9, 2007.
Kerr, Orin S. "Ex Ante Regulation of Computer Search and Seizure" (2010), 96 *Va. L. Rev.* 1241.
Kerr, Orin S. "Searches and Seizures in a Digital World" (2005), 119 *Harv. L. Rev.* 531.
LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 5th ed., vol. 2. St. Paul, Minn.: West, 2012.
Robinton, Lily R. "Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence" (2010), 12 *Yale J.L. & Tech.* 311.

Jurisprudence

Arrêts appliqués : *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145; *R. c. Grant*, 2009 CSC 32, [2009] 2 R.C.S. 353; **arrêts mentionnés :** *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992; *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253; *R. c. Shiers*, 2003 NSCA 138, 219 N.S.R. (2d) 196; *R. c. Sanchez* (1994), 93 C.C.C. (3d) 357; *R. c. Allain* (1998), 205 R.N.-B. (2e) 201; *R. c. E. Star International Inc.*, 2009 ONCJ 576 (CanLII); *BGI Atlantic Inc. c. Canada (Minister of Fisheries and Oceans)*, 2004 NLSCTD 165, 241 Nfld. & P.E.I.R. 206; *R. c. Charles*, 2012 ONSC 2001, 258 C.R.R. (2d) 33; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34; *R. c. Plant*, [1993] 3 R.C.S. 281; *R. c. Mohamad* (2004), 69 O.R. (3d) 481; *R. c. Boudreau-Fontaine*, 2010 QCCA 1108 (CanLII); *Descôteaux c. Mierzwinski*, [1982] 1 R.C.S. 860; *Lavallee, Rackel & Heintz c. Canada (Procureur général)*, 2002 CSC 61, [2002] 3 R.C.S. 209; *United States c. Carey*, 172 F.3d 1268 (1999); *United States c. Burgess*, 576 F.3d 1078 (2009); *United States c. Christie*, 717 F.3d 1156 (2013); *R. c. Côté*, 2011 CSC 46, [2011] 3 R.C.S. 215.

Lois et règlements cités

Charte canadienne des droits et libertés, art. 8, 24(2).
Code criminel, L.R.C. 1985, ch. C-46, art. 186(4)*d*), 326(1)*a*), 487, 487.1, 488, 488.1.
Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5.

Doctrine et autres documents cités

Fontana, James A., and David Keeshan. *The Law of Search and Seizure in Canada*, 8th ed. Markham, Ont. : LexisNexis, 2010.
Gold, Alan D. « Applying Section 8 in the Digital World : Seizures and Searches ». Paper prepared for the Law Society of Upper Canada, 7th Annual Six-Minute Criminal Defence Lawyer, June 9, 2007.
Kerr, Orin S. « Ex Ante Regulation of Computer Search and Seizure » (2010), 96 *Va. L. Rev.* 1241.
Kerr, Orin S. « Searches and Seizures in a Digital World » (2005), 119 *Harv. L. Rev.* 531.
LaFave, Wayne R. *Search and Seizure : A Treatise on the Fourth Amendment*, 5th ed., vol. 2. St. Paul, Minn. : West, 2012.
Robinton, Lily R. « Courting Chaos : Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence » (2010), 12 *Yale J.L. & Tech.* 311.

APPEAL from a judgment of the British Columbia Court of Appeal (Low, Levine and Frankel JJ.A.), 2011 BCCA 536, 315 B.C.A.C. 36, 535 W.A.C. 36, 92 C.R. (6th) 15, 250 C.R.R. (2d) 108, 285 C.C.C. (3d) 160, [2011] B.C.J. No. 2487 (QL), 2011 CarswellBC 3551, setting aside the acquittals entered by Bruce J., 2010 BCSC 2012, [2010] B.C.J. No. 2963 (QL), 2010 CarswellBC 4018, and ordering a new trial. Appeal dismissed.

Elizabeth P. Lewis, *Neil L. Cobb* and *Nancy Seto*, for the appellant.

W. Paul Riley and *Martha M. Devlin*, *Q.C.*, for the respondent.

Michal Fairburn and *Lisa Henderson*, for the intervener the Attorney General of Ontario.

Jolaine Antonio, for the intervener the Attorney General of Alberta.

Nader R. Hasan and *Gerald J. Chan*, for the intervener the British Columbia Civil Liberties Association.

David S. Rose and *Allan Manson*, for the intervener the Canadian Civil Liberties Association.

Paul J. I. Alexander, for the intervener the Criminal Lawyers' Association (Ontario).

The judgment of the Court was delivered by

CROMWELL J. —

I. Introduction

[1] In this case, the digital and Internet age meets the law of search and seizure. The encounter raises a novel issue: Does the traditional legal framework require some updating in order to protect the unique privacy interests that are at stake in computer searches? The traditional legal framework

POURVOI contre un arrêt de la Cour d'appel de la Colombie-Britannique (les juges Low, Levine et Frankel), 2011 BCCA 536, 315 B.C.A.C. 36, 535 W.A.C. 36, 92 C.R. (6th) 15, 250 C.R.R. (2d) 108, 285 C.C.C. (3d) 160, [2011] B.C.J. No. 2487 (QL), 2011 CarswellBC 3551, qui a annulé les acquittements prononcés par la juge Bruce, 2010 BCSC 2012, [2010] B.C.J. No. 2963 (QL), 2010 CarswellBC 4018, et qui a ordonné la tenue d'un nouveau procès. Pourvoi rejeté.

Elizabeth P. Lewis, *Neil L. Cobb* et *Nancy Seto*, pour l'appelant.

W. Paul Riley et *Martha M. Devlin*, *c.r.*, pour l'intimée.

Michal Fairburn et *Lisa Henderson*, pour l'intervenant le procureur général de l'Ontario.

Jolaine Antonio, pour l'intervenant le procureur général de l'Alberta.

Nader R. Hasan et *Gerald J. Chan*, pour l'intervenante l'Association des libertés civiles de la Colombie-Britannique.

David S. Rose et *Allan Manson*, pour l'intervenante l'Association canadienne des libertés civiles.

Paul J. I. Alexander, pour l'intervenante Criminal Lawyers' Association (Ontario).

Version française du jugement de la Cour rendu par

LE JUGE CROMWELL —

I. Introduction

[1] Dans la présente affaire, l'ère du numérique et d'Internet rencontre le droit relatif aux fouilles, perquisitions et saisies. Cette rencontre soulève une question inédite : Est-il nécessaire de procéder à une certaine actualisation du cadre juridique traditionnel afin de protéger les intérêts uniques en matière

holds that once police obtain a warrant to search a place for certain things, they can look for those things anywhere in the place where they might reasonably be; the police do not require specific, prior authorization to search in receptacles such as cupboards and filing cabinets. The question before us is whether this framework is appropriate for computer searches; in short, should our law of search and seizure treat a computer as if it were a filing cabinet or a cupboard?

[2] In my view, it should not. Computers differ in important ways from the receptacles governed by the traditional framework and computer searches give rise to particular privacy concerns that are not sufficiently addressed by that approach. One cannot assume that a justice who has authorized the search of a place has taken into account the privacy interests that might be compromised by the search of any computers found within that place. This can only be assured if, as is my view, the computer search requires specific pre-authorization.

[3] In practical terms, the requirement of specific, prior authorization means that if police intend to search computers found within a place with respect to which they seek a warrant, they must satisfy the authorizing justice that they have reasonable grounds to believe that any computers they discover will contain the things they are looking for. If, in the course of a warranted search, police come across a computer that may contain material for which they are authorized to search but the warrant does not give them specific, prior authorization to search computers, they may seize the device but must obtain further authorization before it is searched.

de vie privée que met en jeu la fouille des ordinateurs? Selon le cadre juridique traditionnel, lorsque des policiers obtiennent un mandat les autorisant à perquisitionner dans un lieu et à y chercher certaines choses, ils peuvent fouiller partout dans ce lieu où ces choses pourraient raisonnablement se trouver. Ils n'ont pas besoin d'obtenir une autorisation expresse préalable pour fouiller dans des contenants tels que des placards et des classeurs. La question dont nous sommes saisis en l'espèce est celle de savoir si ce cadre juridique convient à la fouille des ordinateurs. Bref, nos règles de droit régissant les fouilles, les perquisitions et les saisies devraient-elles traiter les ordinateurs comme s'il s'agissait de classeurs ou de placards?

[2] À mon sens, elles ne devraient pas. Les ordinateurs diffèrent à bien des égards des contenants visés par le cadre juridique traditionnel, et la fouille des ordinateurs soulève, en matière de respect de la vie privée, des préoccupations particulières dont ne tient pas suffisamment compte cette approche traditionnelle. On ne saurait présumer que le juge de paix ayant autorisé des policiers à perquisitionner dans un lieu a pris en compte les intérêts en matière de vie privée auxquels pourrait porter atteinte la fouille des ordinateurs trouvés dans ce lieu. Le seul moyen propre à assurer la prise en compte de ces intérêts consiste selon moi à exiger que la fouille d'un ordinateur fasse l'objet d'une autorisation expresse préalable.

[3] En pratique, voici ce que signifie l'obligation d'obtenir une autorisation expresse préalable : si les policiers ont l'intention de fouiller les ordinateurs se trouvant dans le lieu à l'égard duquel ils sollicitent un mandat, ils doivent convaincre le juge de paix saisi de la demande d'autorisation qu'ils ont des motifs raisonnables de croire que tout ordinateur qu'ils pourraient y trouver contiendra les choses qu'ils recherchent. Si, dans le cours d'une perquisition avec mandat, les policiers trouvent un ordinateur susceptible de contenir des éléments qu'ils sont autorisés à rechercher, et que le mandat dont ils disposent ne les autorise pas de manière expresse et préalable à fouiller des ordinateurs, ils peuvent saisir l'appareil, mais doivent obtenir une autre autorisation avant de le fouiller.

II. Overview and Issues

[4] The appellant was charged with production of marijuana, possession of marijuana for the purpose of trafficking, and theft of electricity. The police obtained a warrant authorizing the search of a residence for evidence of theft of electricity, including documentation identifying the owners and/or occupants of the residence. Even though the Information to Obtain a Search Warrant ("ITO") indicated that the police intended to search for, among other things, "computer generated notes", the warrant did not specifically refer to computers or authorize the search of computers: A.R., vol. II, at p. 112. In the course of their search of the residence, police found marijuana and they also discovered two computers and a cellular telephone. A search of these devices led to evidence that the appellant was the occupant of the residence.

[5] At trial, the appellant claimed that these searches violated his rights under s. 8 of the *Canadian Charter of Rights and Freedoms* and asked the judge to exclude the evidence found as a result. The judge concluded that the ITO did not establish reasonable grounds to believe that documentation identifying the owners and/or occupants would be found in the residence and so the warrant could not authorize the search for such documents. In addition, the trial judge found that police were not authorized to search the personal computers and cellular telephone because those devices were not specifically mentioned in the warrant. She excluded most of the evidence found as a result of these searches and acquitted the accused of the drug charges (2010 BCSC 2012 (CanLII)).

[6] The Crown appealed and the Court of Appeal set aside the acquittals and ordered a new trial (2011 BCCA 536, 315 B.C.A.C. 36). In the court's view, the warrant had properly authorized the searches and there had been no breach of the appellant's s. 8 *Charter* rights.

II. Aperçu et questions en litige

[4] L'appelant a été accusé de production de marijuana, de possession de marijuana en vue d'en faire le trafic et de vol d'électricité. Les policiers ont obtenu un mandat les autorisant à perquisitionner dans une résidence pour y rechercher des preuves de vol d'électricité, y compris des documents identifiant les propriétaires et/ou occupants de la résidence. Même si la Dénonciation en vue d'obtenir un mandat de perquisition (« Dénonciation ») indiquait que les policiers entendaient chercher notamment [TRADUCTION] « des notes générées par ordinateur », le mandat ne faisait pas expressément mention des ordinateurs et n'autorisait pas non plus la fouille de tels appareils : d.a., vol. II, p. 112. Durant la perquisition dans la résidence, les policiers ont trouvé de la marijuana, en plus de découvrir deux ordinateurs et un téléphone cellulaire. La fouille de ces appareils a permis de découvrir des éléments de preuve établissant que l'appelant était l'occupant de la résidence.

[5] Au procès, l'appelant a soutenu que ces fouilles avaient violé les droits que lui garantit l'art. 8 de la *Charte canadienne des droits et libertés*, et il a demandé à la juge d'exclure les éléments de preuve ainsi découverts. Celle-ci a conclu que la Dénonciation ne démontrait pas l'existence de motifs raisonnables de croire que des documents identifiant les propriétaires et/ou occupants se trouveraient dans la résidence, et qu'en conséquence le mandat ne pouvait autoriser la recherche de tels documents. La juge de première instance a en outre conclu que les policiers n'étaient pas autorisés à fouiller les ordinateurs personnels et le téléphone cellulaire, parce que ces appareils n'étaient pas expressément mentionnés dans le mandat. Elle a écarté la plupart des éléments de preuve découverts par suite de ces fouilles, et elle a acquitté l'accusé des accusations liées à la drogue (2010 BCSC 2012 (CanLII)).

[6] Le ministère public a interjeté appel et la Cour d'appel a annulé les acquittements et ordonné la tenue d'un nouveau procès (2011 BCCA 536, 315 B.C.A.C. 36). De l'avis de la Cour d'appel, le mandat avait dûment autorisé les fouilles et il n'y avait eu aucune violation des droits garantis à l'appelant par l'art. 8 de la *Charte*.

[7] The appellant's further appeal to this Court raises three issues:

1. Did the search warrant properly permit a search for documentation identifying the owners and/or occupants?

2. Did the warrant authorize the search of the computers and cellular telephone?

3. If the search was unlawful, should the evidence obtained be excluded?

[8] On the first issue, I agree with the Court of Appeal that the ITO established reasonable grounds to believe that relevant documents would be found in the residence. It follows that the warrant properly authorized a search for that sort of material. On the second issue, I agree with the trial judge that the warrant did not authorize the search of the computers and cellular telephone. However, I conclude that the trial judge was wrong to exclude the evidence found as a result. I would therefore dismiss the appeal.

III. Analysis

A. *First Issue: Reasonable Grounds to Search for Ownership or Occupancy Documentation*

[9] I agree with the Court of Appeal that the facts provided in the ITO were sufficient to support a reasonable inference on the part of the issuing justice that documentation evidencing ownership or occupancy would be found in the residence. The trial judge, in concluding otherwise, did not show sufficient deference to the issuing justice's assessment of the evidence. Some background about the ITO and the decisions at trial and on appeal helps to explain my conclusion.

[7] Le pourvoi formé par l'appelant devant notre Cour soulève trois questions :

1. Le mandat de perquisition autorisait-il dûment la recherche de documents identifiant les propriétaires et/ou occupants?

2. Le mandat autorisait-il la fouille des ordinateurs et du téléphone cellulaire?

3. Si la fouille était illégale, la preuve obtenue devait-elle être écartée?

[8] Pour ce qui est de la première question, je souscris à la conclusion de la Cour d'appel selon laquelle la Dénonciation démontrait l'existence de motifs raisonnables de croire que des documents pertinents se trouveraient dans la résidence. Il s'ensuit que le mandat autorisait dûment la recherche de documents de cette nature. Quant à la deuxième question, à l'instar de la juge de première instance, j'estime que le mandat n'autorisait pas la fouille des ordinateurs et du téléphone cellulaire. Toutefois, je conclus que la juge a eu tort d'écarter les éléments de preuve ainsi découverts par suite de cette fouille. Je rejetterais donc le pourvoi.

III. Analyse

A. *Première question : motifs raisonnables de rechercher des documents confirmant l'identité des propriétaires ou occupants*

[9] Je fais mienne la conclusion de la Cour d'appel selon laquelle les faits énoncés dans la Dénonciation étaient suffisants pour permettre au juge de paix qui a décerné le mandat d'inférer raisonnablement que des documents confirmant l'identité des propriétaires ou occupants seraient trouvés dans la résidence. Or, en tirant une conclusion différente, la juge de première instance n'a pas manifesté suffisamment de déférence envers l'appréciation de la preuve par le juge de paix. Un certain nombre de renseignements sur le contexte de la Dénonciation et des décisions rendues au procès et en appel aideront à expliquer ma propre conclusion.

[10] On August 31, 2007, Mr. Hall, a subcontractor of British Columbia Hydro, informed police that a service check of the hydro meter outside premises on 84 Avenue in Langley showed that electricity was being diverted and used without being recorded for billing purposes. B.C. Hydro records listed Foh Hiong as the subscriber for the electrical service at the property. Having received this information, Constable Carter searched the RCMP computer system and determined that the current owner of the residence was Thanh L. Vu. He found that there was no homeowner grant being claimed for the residence and there was no business licence associated with it. Cst. Carter drove by the residence and made observations of its style (a two-storey house with a basement) and address as well as the location of the hydro-meter. He contacted Mr. Hall on September 6, 2007, to confirm that: no B.C. Hydro employee had removed any hydro-electrical diversion from the residence; Mr. Hall still believed a theft of electricity was ongoing; and the subscriber's name on the B.C. Hydro account was still the same. Using this information, Cst. Carter swore an ITO for the premises for the purpose of locating evidence of a theft of electricity.

[11] The ITO indicated that Cst. Carter intended to seize any evidence supporting a charge of theft of electricity contrary to s. 326(1)(*a*) of the *Criminal Code*, R.S.C. 1985, c. C-46. In particular, he intended to seize all equipment and parts utilized to divert electricity, including: ". . . meter bases, the electrical meters, new and used BC Hydro meter seals, typed, written or computer generated notes relative to the theft of the hydro electricity and records and documentation relating to occupancy and control over the property and electrical services supplied": A.R., vol. II, at p. 112.

[10] Le 31 août 2007, M. Hall, un sous-traitant de British Columbia Hydro, a informé la police qu'une vérification du compteur d'électricité extérieur d'une propriété située sur l'avenue 84 à Langley avait révélé que de l'électricité était détournée et utilisée sans que cette consommation soit enregistrée et facturée. Les dossiers de B.C. Hydro indiquaient que l'abonné aux services d'électricité pour la propriété s'appelait Foh Hiong. Après avoir reçu ces renseignements, l'agent Carter a effectué des recherches dans le système informatique de la GRC et déterminé que le propriétaire de la résidence se nommait Thanh L. Vu. Il a aussi constaté qu'aucune subvention aux propriétaires n'était réclamée à l'égard de la résidence et que celle-ci ne faisait l'objet d'aucun permis d'exploitation commerciale. L'agent Carter est ensuite passé en voiture devant la résidence et a noté des observations sur le type de construction de celle-ci (maison à deux étages avec sous-sol), son adresse ainsi que l'emplacement du compteur. Le 6 septembre 2007, il a communiqué avec M. Hall pour obtenir la confirmation de ce qui suit : aucun employé de B.C. Hydro n'avait enlevé de dispositifs de détournement d'hydro-électricité de la résidence; M. Hall croyait encore qu'un vol d'électricité continuait d'avoir lieu; le nom de l'abonné sur le compte de B.C. Hydro était toujours le même. S'appuyant sur ces renseignements, l'agent Carter a préparé une dénonciation sous serment en vue d'obtenir un mandat de perquisition visant les lieux en question afin d'y rechercher des éléments de preuve de vol d'électricité.

[11] La Dénonciation indiquait que l'agent Carter entendait saisir tout élément de preuve étayant une accusation de vol d'électricité en violation de l'al. 326(1)*a*) du *Code criminel*, L.R.C. 1985, ch. C-46. En particulier, il entendait saisir tout équipement ou composant utilisé pour détourner l'électricité, y compris : [TRADUCTION] « . . . les socles, les compteurs d'électricité, les sceaux — neufs et usagés — du compteur de B.C. Hydro, les notes dactylographiées, manuscrites ou générées par ordinateur se rapportant au vol d'électricité, ainsi que les relevés et documents relatifs à l'occupation de la propriété et au contrôle exercé sur celle-ci et les services électriques fournis » : d.a., vol. II, p. 112.

[12] A Justice of the Peace issued a search warrant authorizing seizure of "[a]ll equipment and parts utilized to divert electricity, including the meter bases, electrical meters, electrical wires, hydro bypass connections [as well as] [d]ocumentation identifying ownership and/or occupancy of the property" relevant to an investigation of the offence: A.R., vol. II, at p. 109.

[13] The appellant argued at trial that the search for documents relating to ownership and occupation violated his rights under s. 8 of the *Charter* to be free from unreasonable searches and seizures. He submitted that the warrant should not have authorized a search for that sort of documentation because the ITO did not set out reasonable grounds to believe that ownership documentation would be found in the residence.

[14] On the *voir dire* at trial, Cst. Carter agreed that the ITO contained no statement concerning his grounds to believe that documents evidencing ownership or occupation would be found in the residence. The trial judge found that "[t]he ITO does not contain a statement by its author that there are reasonable grounds to believe that documents evidencing ownership or occupation will be found in the Residence. Nor does the ITO contain any facts to support such a belief by Cst. Carter who drafted the ITO" (*voir dire* decision, 2010 BCSC 1260, 218 C.R.R. (2d) 98, at para. 54). She concluded therefore that the ITO could not support a search warrant for documents evidencing ownership or occupation (para. 54).

[15] The Court of Appeal found that this was an error. According to the court, the trial judge had reweighed the grounds set out in the ITO and substituted her view of the sufficiency of the evidence

[12] Un juge de paix a délivré un mandat de perquisition autorisant la saisie de [TRADUCTION] « [t]out équipement ou composant utilisé pour détourner l'électricité, y compris les socles, les compteurs d'électricité, les fils électriques, les dispositifs de détournement d'électricité [ainsi que] [l]es documents identifiant les propriétaires et/ou occupants de la propriété » pertinents pour les besoins d'une enquête sur l'infraction : d.a., vol. II, p. 109.

[13] Au procès, l'appelant a plaidé que les fouilles effectuées pour chercher des documents permettant d'identifier les propriétaires et occupants avaient violé le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives que lui garantit l'art. 8 de la *Charte*. Il a soutenu que le mandat n'aurait pas dû autoriser les policiers à procéder à des fouilles visant des documents de cette nature, étant donné que la Dénonciation ne faisait pas état de motifs raisonnables de croire que des documents relatifs à l'identité des propriétaires seraient découverts dans la résidence.

[14] Lors du voir-dire au procès, l'agent Carter a reconnu que la Dénonciation ne renfermait aucune déclaration concernant les motifs pour lesquels il croyait que des documents confirmant l'identité des propriétaires ou occupants seraient découverts dans la résidence. La juge de première instance a conclu que [TRADUCTION] « [l]a Dénonciation ne contient aucune déclaration de son auteur indiquant qu'il existe des motifs raisonnables de croire que des documents confirmant l'identité des propriétaires ou occupants seront découverts dans la résidence. La Dénonciation ne mentionne pas non plus de faits appuyant la conviction de l'agent Carter à cet égard, l'auteur de la Dénonciation » (décision sur le voir-dire, 2010 BCSC 1260, 218 C.R.R. (2d) 98, par. 54). Elle a en conséquence conclu que la Dénonciation ne pouvait justifier la délivrance d'un mandat de perquisition permettant de chercher des documents confirmant l'identité des propriétaires ou occupants (par. 54).

[15] La Cour d'appel a jugé qu'il s'agissait là d'une erreur. Selon elle, la juge de première instance avait réévalué les motifs énoncés dans la Dénonciation et substitué son opinion sur le

for that of the issuing justice. In my respectful view, the Court of Appeal was on firm ground in reaching this conclusion.

[16] The question for the reviewing judge is "whether there was reliable evidence that might reasonably be believed on the basis of which the authorization could have issued, not whether in the opinion of the reviewing judge, the application should have been granted at all by the authorizing judge": *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992, at para. 54 (emphasis deleted); *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 40. In applying this test, the reviewing judge must take into account that authorizing justices may draw reasonable inferences from the evidence in the ITO; the informant need not underline the obvious: *R. v. Shiers*, 2003 NSCA 138, 219 N.S.R. (2d) 196, at para. 13; *R. v. Sanchez* (1994), 93 C.C.C. (3d) 357 (Ont. Ct. (Gen. Div.)), at pp. 364-65; *R. v. Allain* (1998), 205 N.B.R. (2d) 201 (C.A.), at para. 11.

[17] The ITO set out facts sufficient to allow the authorizing justice to reasonably draw the inference that there were reasonable grounds to believe that documents evidencing ownership or occupation would be found in the residence: A.R., vol. II, at p. 112. In particular, the ITO referred to the premises to be searched as a "residence" and as a "two (2) story house" (p. 111). It also indicated that the appellant owned the property and that electricity was being consumed there (pp. 110-11). In my view, it is a reasonable inference that a residence would be the place to look for documents evidencing ownership or occupation. Where else would one expect to find such documents if not in the residence itself? Moreover, I think that the authorizing justice could reasonably infer that a place was being occupied as a residence from the fact that electricity was being consumed at that place and that it had an owner.

caractère suffisant de la preuve à celle du juge de paix qui avait décerné le mandat. À mon humble avis, cette conclusion de la Cour d'appel reposait sur de solides assises.

[16] Le juge qui siège en révision doit trancher la question de savoir « s'il existait quelque élément de preuve fiable auquel le juge aurait pu raisonnablement ajouter foi pour accorder l'autorisation, et non si, de l'avis du juge siégeant en révision, le juge saisi de la demande d'autorisation aurait dû y faire droit » : *R. c. Araujo*, 2000 CSC 65, [2000] 2 R.C.S. 992, par. 54 (soulignement omis); *R. c. Morelli*, 2010 CSC 8, [2010] 1 R.C.S. 253, par. 40. En appliquant ce critère, le juge siégeant en révision doit se rappeler que le juge de paix saisi de la demande d'autorisation peut tirer des inférences raisonnables de la preuve présentée dans la dénonciation; l'auteur de la dénonciation n'est pas tenu de souligner à grands traits ce qui est par ailleurs évident : *R. c. Shiers*, 2003 NSCA 138, 219 N.S.R. (2d) 196, par. 13; *R. c. Sanchez* (1994), 93 C.C.C. (3d) 357 (C. Ont. (Div. gén.)), p. 364-365; *R. c. Allain* (1998), 205 R.N.-B. (2e) 201 (C.A.), par. 11.

[17] La Dénonciation énonçait suffisamment de faits pour permettre au juge de paix saisi de la demande d'autorisation d'inférer raisonnablement qu'il existait des motifs raisonnables de croire que des documents confirmant l'identité des propriétaires ou occupants seraient découverts dans la résidence : d.a., vol. II, p. 112. En particulier, la Dénonciation décrivait les lieux visés par la perquisition comme étant une [TRADUCTION] « résidence » et une « maison à deux (2) étages » (p. 111). Elle indiquait également que l'appelant était le propriétaire des lieux et que de l'électricité y était consommée (p. 110-111). À mon avis, il est raisonnable d'inférer qu'une résidence est l'endroit où il faut regarder pour trouver des documents confirmant l'identité de ses propriétaires ou occupants. À quel autre endroit pourrait-on s'attendre à trouver de tels documents, si ce n'est dans la résidence elle-même? Qui plus est, j'estime qu'il était raisonnable pour le juge de paix saisi de la demande d'autorisation d'inférer que la propriété était occupée en tant que résidence, compte tenu du fait que de l'électricité était consommée dans ce lieu et que celui-ci avait un propriétaire.

[18] I therefore conclude that the authorizing justice could lawfully issue the warrant to search for documents evidencing ownership or occupation of the property. The search for such material did not breach the appellant's rights under s. 8 of the *Charter*.

B. *Second Issue: The Computer Searches*

1. Introduction

[19] I have concluded that the search warrant authorized the police to search for documentation identifying ownership and occupancy. The next issue is whether the warrant permitted the police to search for that sort of documentation on the computers and cellular telephone found in the residence.

[20] The appellant says that a computer search requires specific pre-authorization in the warrant. The Crown maintains that this is not necessary because after-the-fact review of the reasonableness of a computer search provides the protection guaranteed by s. 8 of the *Charter*. I agree with the appellant.

[21] Section 8 of the *Charter* — which gives everyone the right to be free of unreasonable searches and seizures — seeks to strike an appropriate balance between the right to be free of state interference and the legitimate needs of law enforcement. In addition to the overriding requirement that a reasonable law must authorize the search, this balance is generally achieved in two main ways.

[22] First, the police must obtain judicial authorization for the search *before* they conduct it, usually in the form of a search warrant. The prior authorization requirement ensures that, before a search is conducted, a judicial officer is satisfied that the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance the goals of law enforcement: *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 160.

[18] Par conséquent, je conclus que le juge de paix saisi de la demande d'autorisation pouvait légalement décerner le mandat de perquisition autorisant la recherche de documents confirmant l'identité des propriétaires ou occupants de la propriété. Les fouilles visant de tels documents n'ont pas violé les droits garantis à l'appelant par l'art. 8 de la *Charte*.

B. *Deuxième question : la fouille des ordinateurs*

1. Introduction

[19] J'ai conclu que le mandat de perquisition autorisait les policiers à rechercher des documents identifiant les propriétaires et les occupants. Il s'agit maintenant de se demander si le mandat permettait aux policiers de chercher ce genre de documents dans les ordinateurs et le téléphone cellulaire trouvés dans la résidence.

[20] L'appelant affirme que la fouille d'un ordinateur doit faire l'objet d'une autorisation expresse préalable dans le mandat. Pour sa part, le ministère public soutient qu'une telle autorisation n'est pas nécessaire, parce que le contrôle a posteriori du caractère non abusif de la fouille d'un ordinateur permet d'assurer la protection garantie par l'art. 8 de la *Charte*. Je partage l'opinion de l'appelant.

[21] L'article 8 de la *Charte* — qui confère à chacun le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives — vise à établir un juste équilibre entre le droit à la protection contre l'ingérence de l'État et la nécessité légitime de faire respecter la loi. En plus de l'exigence primordiale selon laquelle la perquisition doit être autorisée par une loi non abusive, cet équilibre est généralement réalisé grâce à deux moyens principaux.

[22] Premièrement, les policiers doivent obtenir des tribunaux l'autorisation d'effectuer la perquisition *avant* de procéder à celle-ci, autorisation qui prend habituellement la forme d'un mandat de perquisition. Cette obligation d'obtenir une autorisation préalable fait en sorte que, avant l'exécution de la perquisition, un officier de justice est convaincu que le droit du public de ne pas être importuné par l'État doit céder le pas au droit de ce dernier de s'immiscer dans la vie privée des particuliers afin

Second, an authorized search must be conducted in a reasonable manner. This ensures that the search is no more intrusive than is reasonably necessary to achieve its objectives. In short, prior authorization *prevents* unjustified intrusions while the requirement that the search be conducted reasonably limits potential abuse of the authorization to search.

de veiller au respect de la loi : *Hunter c. Southam Inc.*, [1984] 2 R.C.S. 145, p. 160. Deuxièmement, la perquisition ainsi autorisée doit être effectuée d'une manière non abusive. Cela permet d'éviter que la perquisition ait un caractère plus envahissant que ce qui est raisonnablement nécessaire pour atteindre ses objectifs. Bref, le fait d'exiger une autorisation préalable *prévient* les intrusions injustifiées, alors que celui d'exiger que la perquisition soit effectuée d'une manière non abusive limite les risques que l'on abuse de l'autorisation de perquisitionner qui a été accordée.

[23] I accept the general proposition, as stated by the Court of Appeal, that "[a] warrant authorizing a search of a specific location for specific things confers on those executing that warrant the authority to conduct a reasonable examination of anything at that location within which the specified things might be found" (para. 63). In other words, specific prior authorization to search anything at that location is not required. The question is whether this general proposition applies to computers or whether specific, prior authorization to search a computer is required.

[23] Je souscris à la proposition générale qu'a formulée dans les termes suivants la Cour d'appel : [TRADUCTION] « Un mandat autorisant une perquisition dans un lieu précis pour chercher des choses précises confère aux personnes qui exécutent ce mandat le pouvoir de procéder à un examen raisonnable de tout élément se trouvant à cet endroit et dans lequel les choses précisées pourraient être découvertes » (par. 63). Autrement dit, une autorisation expresse préalable de fouiller tout ce qui se trouve dans le lieu en question n'est pas requise. Toutefois, la question qui se pose consiste à décider si cette proposition générale s'applique aux ordinateurs ou si la fouille d'un ordinateur requiert l'obtention d'une autorisation expresse préalable.

[24] The privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets. Computers potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search. These factors, understood in light of the purposes of s. 8 of the *Charter*, call for specific pre-authorization in my view.

[24] Les intérêts en matière de respect de la vie privée que met en jeu la fouille des ordinateurs diffèrent nettement de ceux en cause lors de la fouille de contenants tels des placards et des classeurs. En effet, les ordinateurs sont susceptibles de donner aux policiers accès à de vastes quantités de données sur lesquelles les utilisateurs n'ont aucune maîtrise, dont ils ne connaissent peut-être même pas l'existence ou dont ils peuvent avoir choisi de se départir, et qui d'ailleurs pourraient fort bien ne pas se trouver concrètement dans le lieu fouillé. Je suis d'avis que, considérés au regard des objectifs visés par l'art. 8 de la *Charte*, ces facteurs commandent l'obtention d'une autorisation expresse préalable.

[25] Although I find that specific, prior authorization was necessary before police could search the devices found within the appellant's residence, I would not accept one of the intervener's submissions that the authorizing justice was required, in this

[25] Bien que je conclue que les policiers devaient obtenir une autorisation expresse préalable avant de pouvoir fouiller les appareils trouvés dans la résidence de l'appelant, je ne puis accepter les observations de l'un des intervenants selon lesquelles

case, to impose a search protocol in advance with conditions limiting the manner of search. While such conditions may be appropriate in some cases, they are not, as a general rule, constitutionally required and were not, in my view, required in this case.

[26] Before turning to my reasons for these conclusions, I must briefly review the facts, decisions and positions of the parties in relation to this issue.

2. Facts, Decisions and Positions of the Parties

(a) *The Search*

[27] On September 6, 2007, Cst. Carter and several other officers entered the residence pursuant to the warrant. A cursory search led to the discovery of marijuana growing in the basement. The officers also found two computers and a cellular telephone in the living room. Cst. Carter searched the first computer, which was connected to a security system that monitored the front of the residence by means of a video camera. Examining the footage stored in the computer, he located images of a black Honda CRV in the driveway of the residence. The RCMP's database confirmed that the appellant was the registered owner of a 2007 black Honda CRV, that he had a B.C. driver's licence, and that he had a registered address on Quintette Crescent in Coquitlam, B.C.

[28] Cst. George searched the second computer which was running an online chat program called MSN. The last user was still signed in and by activating the MSN icon and bringing up the open file Cst. George was able to see that the user was signed in with the email address raymondvu@hotmail.com. A Facebook account in the name of Raymond Vu was also open. Cst. George searched the computer's database for photographs by using the "Start" menu and the "Search" function which permits a search for any photographs or video files. He also searched for any relevant documents on MS-DOS

le juge de paix saisi de la demande d'autorisation était tenu, dans le présent cas, d'imposer à l'avance un protocole de perquisition assorti de conditions limitant la façon de procéder à la fouille. Quoique de telles conditions puissent convenir dans certains cas, elles ne sont pas, en règle générale, requises par la Constitution et, à mon sens, elles n'étaient pas nécessaires en l'espèce.

[26] Avant d'exposer les motifs au soutien de ces conclusions, je vais examiner brièvement les faits, les décisions et les thèses des parties relativement à cette question.

2. Faits, décisions et thèses des parties

a) *La perquisition*

[27] Le 6 septembre 2007, l'agent Carter et plusieurs autres agents sont entrés dans la résidence sous l'autorité du mandat. Une fouille sommaire a permis de découvrir une culture de marijuana au sous-sol. Les agents ont également trouvé deux ordinateurs et un téléphone cellulaire dans le salon. L'agent Carter a fouillé le premier ordinateur, lequel était connecté à un système de sécurité qui surveillait le devant de la résidence au moyen d'une caméra vidéo. En examinant la vidéo archivée dans l'ordinateur, il a repéré des images d'une Honda CRV noire dans l'entrée de la résidence. La base de données de la GRC a confirmé que l'appelant était enregistré à titre de propriétaire d'une Honda CRV noire 2007, qu'il était titulaire d'un permis de conduire de la C.-B. et qu'il possédait une adresse légale sur Quintette Crescent à Coquitlam, en C.-B.

[28] L'agent George a fouillé le second ordinateur sur lequel un logiciel de clavardage en ligne appelé MSN était en marche. Le dernier utilisateur était toujours connecté et, en activant l'icône MSN et en cliquant sur le document ouvert, l'agent George a pu voir que l'utilisateur était connecté au moyen de l'adresse électronique raymondvu@hotmail.com. Un compte Facebook au nom de Raymond Vu était également ouvert. En utilisant le menu « Démarrer » et la fonction « Rechercher », laquelle permet de rechercher des documents photo ou vidéo, l'agent a aussi fouillé dans la base de données de l'ordinateur

or WordPerfect. The search turned up the résumé of Raymond Vu, of which another officer took a photograph. Cst. George did not take many notes during his search and could not recall the steps he took in the process.

[29] On October 18, 2007, Cst. George obtained the serial number for a computer modem found at the residence and filed a request under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, to obtain the name of the subscriber. His report to the Crown indicated that the subscriber was Luan Vu, although Cst. George acknowledged that this person was not a current subscriber.

[30] Cst. Carter searched the Sony Ericsson model cellular telephone found in the living room. Stored in the phone's database, he discovered a photo of an Asian male, whom Cst. Carter identified as the appellant.

[31] Cst. MacNeil was the exhibits officer for the search. He seized the two computers, the cellular telephone, a power cord for the phone, and a zip drive (a portable computer storage device). He applied for and obtained a detention order to permit the RCMP to retain the two computers and the cellular telephone. The detention order was valid for a period of 90 days unless charges were laid before its expiry.

[32] On January 6, 2008, a few days after the detention order had expired, Sgt. Wilde carried out a second search of the security computer. Cst. George had made a DVD of all the footage in the database but it had been lost. Sgt. Wilde prepared a number of still shots which depicted a vehicle arriving at the residence and a male attending the residence in the five days preceding the execution of the search warrant. Sgt. Wilde admitted that he intentionally had not made any notes of his search of the

à la recherche de photos. Il a également recherché tout document pertinent dans MS-DOS ou WordPerfect. Cette recherche a permis de découvrir le curriculum vitae de Raymond Vu, dont un autre agent a pris une photo. L'agent George n'a pas pris beaucoup de notes durant sa fouille et il ne pouvait se souvenir des différentes opérations qu'il avait effectuées à l'occasion de celle-ci.

[29] Le 18 octobre 2007, l'agent George a obtenu le numéro de série d'un modem d'ordinateur trouvé dans la résidence et il a déposé, en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, une demande en vue d'obtenir le nom de l'abonné. Dans le rapport qu'il a présenté au ministère public, il a indiqué que l'abonné s'appelait Luan Vu, reconnaissant toutefois que cette personne n'était pas un abonné à ce moment.

[30] L'agent Carter a fouillé le téléphone cellulaire (de modèle Sony Ericsson) trouvé dans le salon de la résidence. Dans la base de données du téléphone, il a découvert la photo d'un homme asiatique, qu'il a identifié comme étant l'appelant.

[31] L'agent MacNeil, qui était l'agent chargé des pièces à conviction lors de la perquisition, a saisi les deux ordinateurs, le téléphone cellulaire, le cordon d'alimentation du téléphone ainsi qu'un lecteur zip (dispositif de stockage portable pour ordinateur). Il a demandé et obtenu une ordonnance de détention pour permettre à la GRC de conserver les deux ordinateurs et le téléphone cellulaire. Cette ordonnance était valide pour 90 jours à moins que des accusations ne soient portées avant l'expiration de cette période.

[32] Le 6 janvier 2008, quelques jours après l'expiration de l'ordonnance de détention, le sergent Wilde a fouillé une deuxième fois l'ordinateur du système de sécurité. L'agent George avait transféré sur un DVD toutes les images figurant dans la base de données, mais ce DVD avait été égaré. Le sergent Wilde a préparé un certain nombre de photos qui montraient un véhicule arrivant à la résidence et un homme se présentant à celle-ci dans les cinq jours qui ont précédé l'exécution du mandat

computers at the residence to ensure he would not have to testify in court about the search.

(b) *Decisions*

[33] The trial judge concluded that the warrant that police had obtained to search the residence did not authorize the search of the laptop computer or the cellular telephone found therein. In her view:

> . . . it is no longer conceivable that a search warrant for a residence could implicitly authorize the search of a computer (or a cellular telephone containing a memory capacity akin to a computer) that may be found in the premises even where the warrant specifically grants an authority to search for documentary evidence of occupation or ownership. [Emphasis deleted; *voir dire* decision, at para. 65.]

[34] The Court of Appeal disagreed with the trial judge's ruling on the *voir dire*. It found that computers and cellular telephones were likely repositories of "[d]ocumentation identifying ownership and/or occupancy of the property", and as such they could be searched under the warrant. The court concluded that there is nothing in the nature of electronic devices that requires the law of search and seizure to treat them differently from other receptacles found on premises for which a search has been authorized.

(c) *Positions of the Parties*

[35] The appellant, with the support of certain interveners, submits that authorization to search a residence for documents does not include authorization to search computers and cellular telephones found in that place. The appellant maintains that searches of these devices engage more important privacy interests than searches of other receptacles that may be found in a place, such as drawers in a

de perquisition. Le sergent Wilde a admis qu'il avait intentionnellement omis de prendre des notes concernant la fouille des ordinateurs à la résidence pour s'assurer de ne pas avoir à témoigner en cour à ce sujet.

b) *Décisions*

[33] La juge de première instance a conclu que le mandat obtenu par les policiers pour perquisitionner à la résidence n'autorisait pas la fouille de l'ordinateur portable et du téléphone cellulaire qui y ont été trouvés. À son avis :

> [TRADUCTION] . . . il n'est désormais plus possible de penser qu'un mandat de perquisition visant une résidence puisse implicitement autoriser la fouille d'un ordinateur (ou d'un téléphone cellulaire comportant une capacité de mémoire semblable à celle d'un ordinateur) qui pourrait être découvert sur les lieux, même lorsque le mandat accorde expressément le pouvoir de chercher des éléments de preuve documentaire confirmant l'identité des occupants ou propriétaires. [Italiques omis; décision sur le voir-dire, par. 65.]

[34] La Cour d'appel n'a pas souscrit à la décision rendue par la juge de première instance au terme du voir-dire. Elle a plutôt conclu que les ordinateurs et téléphones cellulaires constituent des endroits où il est plausible que soient conservés des [TRADUCTION] « documents identifiant les propriétaires et/ou occupants de la propriété » et, pour cette raison, qu'ils peuvent être fouillés en vertu du mandat. La Cour d'appel a également jugé que rien dans la nature des appareils électroniques n'a pour effet d'exiger que le droit relatif aux fouilles, perquisitions et saisies traite ces appareils différemment des autres contenants trouvés dans des lieux où une perquisition a été autorisée.

c) *Thèses des parties*

[35] L'appelant soutient, avec l'appui de certains intervenants, qu'une autorisation de fouiller une résidence en vue d'y chercher des documents n'emporte pas l'autorisation de fouiller les ordinateurs et les téléphones cellulaires découverts dans cet endroit. Il affirme que la fouille de tels appareils met en jeu des intérêts plus importants en matière de vie privée que la fouille d'autres contenants

desk or a filing cabinet. These unique features challenge the efficacy of standard limitations on searches articulated in terms of place, time, and subject matter. The appellant therefore submits that specific authorization is required before police can search a computer.

[36] In contrast, the Crown maintains that established principles of search and seizure are sufficient to meet the challenges posed by new technologies; there is no need for a special regime requiring specific authorization for "computer searches": R.F., at para. 93. If a warrant authorizes the search of a place for documents, police are authorized to search computers found in that place if those computers might reasonably contain the documents for which the search was authorized. A special regime for computer searches is not advisable because technology is constantly changing and not all computers are used in a manner that engages important privacy interests. Moreover, computer searches are not all alike and different principles of search and seizure may be engaged depending on the circumstances in which the authorities encounter a computer. The Crown warns that requiring specific authority to search computers would restrict access to valuable information and undermine legitimate investigations.

3. Authorizing the Search of Computers Found in a Place of Search

[37] I agree with the appellant and the trial judge that computer searches require specific, prior authorization.

[38] I do not distinguish, for the purposes of prior authorization, the computers from the cellular telephone in issue here. Although historically cellular telephones were far more restricted than

susceptibles de se trouver dans un lieu, par exemple les tiroirs d'un bureau ou d'un classeur. Ces caractéristiques uniques compromettent l'efficacité des restrictions qui sont normalement imposées quant au lieu, à la durée et à l'objet d'une perquisition. En conséquence, l'appelant prétend que les policiers doivent obtenir une autorisation expresse avant de pouvoir fouiller un ordinateur.

[36] En revanche, le ministère public plaide que les principes bien établis du droit relatif aux fouilles, perquisitions et saisies permettent de répondre aux défis que soulèvent les nouvelles technologies; qu'il n'est pas nécessaire d'instituer un régime particulier exigeant l'obtention d'une autorisation expresse pour [TRADUCTION] « les fouilles d'ordinateurs » : m.i., par. 93. Si un mandat autorise les policiers à perquisitionner dans un lieu en vue d'y chercher des documents, ces derniers sont autorisés à fouiller les ordinateurs découverts dans ce lieu si ces appareils peuvent raisonnablement contenir les documents à l'égard desquels la perquisition a été autorisée. Il ne serait pas souhaitable d'instaurer un régime particulier pour les fouilles d'ordinateurs, car la technologie évolue constamment et les ordinateurs ne sont pas tous utilisés d'une manière qui soulève des intérêts importants en matière de respect de la vie privée. De plus, les fouilles d'ordinateurs ne sont pas toutes pareilles, et différents principes relatifs aux fouilles, perquisitions et saisies peuvent entrer en jeu selon les circonstances dans lesquelles les autorités trouvent des ordinateurs. Le ministère public souligne que le fait d'exiger une autorisation expresse à l'égard de la fouille des ordinateurs limiterait l'accès à des renseignements très utiles et compromettrait des enquêtes légitimes.

3. Autorisation de fouiller les ordinateurs découverts dans un lieu perquisitionné

[37] Tout comme l'appelant et la juge de première instance, je suis d'avis que la fouille d'un ordinateur exige l'obtention d'une autorisation expresse préalable.

[38] En ce qui a trait à l'autorisation préalable, je ne fais aucune distinction entre les ordinateurs et le téléphone cellulaire en litige dans la présente affaire. Il est vrai que, dans le passé, le volume et le genre

computers in terms of the amount and kind of information that they could store, present day phones have capacities that are, for our purposes, equivalent to those of computers. The trial judge found that the cellular telephone in this case, for example, had a "memory capacity akin to a computer": *voir dire* decision, at para. 65. In these reasons, then, when I referred to "computers", I include within that term the cellular telephone.

(a) *Specific, Prior Authorization Is Required for Computer Searches*

[39] As noted earlier, the general principle is that authorization to search a place includes authorization to search places and receptacles within that place: J. A. Fontana and D. Keeshan, *The Law of Search and Seizure in Canada* (8th ed. 2010), at p. 1181; see, for example, *R. v. E. Star International Inc.*, 2009 ONCJ 576 (CanLII), at para. 17; *BGI Atlantic Inc. v. Canada (Minister of Fisheries and Oceans)*, 2004 NLSCTD 165, 241 Nfld. & P.E.I.R. 206, at paras. 70-72; *R. v. Charles*, 2012 ONSC 2001, 258 C.R.R. (2d) 33, at para. 61. This general rule is based on the assumption that, if the search of a place for certain things is justified, so is the search for those things in receptacles found within that place. However, this assumption is *not* justified in relation to computers because computers are not like other receptacles that may be found in a place of search. The particular nature of computers calls for a specific assessment of whether the intrusion of a computer search is justified, which in turn requires prior authorization.

(i) Computers Are Different From Other "Receptacles"

[40] It is difficult to imagine a more intrusive invasion of privacy than the search of a personal or home computer: *Morelli*, at para. 105; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at para. 3. Computers are

de données qu'il était possible de stocker dans les téléphones cellulaires étaient bien plus limités que dans les ordinateurs, mais les cellulaires modernes disposent de capacités qui, pour les fins qui nous occupent, équivalent à celles des ordinateurs. La juge de première instance a conclu que, par exemple, le téléphone cellulaire saisi en l'espèce possédait [TRADUCTION] « une capacité de mémoire analogue à celle d'un ordinateur » : décision sur le voir-dire, par. 65. Par conséquent, lorsque je fais mention des « ordinateurs » dans les présents motifs, je vise également le téléphone cellulaire.

a) *Nécessité d'une autorisation expresse préalable en cas de fouille d'ordinateurs*

[39] Comme il a été indiqué précédemment, suivant le principe général applicable, l'autorisation de perquisitionner dans un lieu emporte celle de fouiller les espaces et contenants se trouvant dans ce lieu : J. A. Fontana et D. Keeshan, *The Law of Search and Seizure in Canada* (8e éd. 2010), p. 1181; voir, par exemple, *R. c. E. Star International Inc.*, 2009 ONCJ 576 (CanLII), par. 17; *BGI Atlantic Inc. c. Canada (Minister of Fisheries and Oceans)*, 2004 NLSCTD 165, 241 Nfld. & P.E.I.R. 206, par. 70-72; *R. c. Charles*, 2012 ONSC 2001, 258 C.R.R. (2d) 33, par. 61. Cette règle générale repose sur l'hypothèse selon laquelle, si l'exécution d'une perquisition dans un lieu pour y chercher certaines choses est justifiée, la recherche de ces choses dans les contenants découverts dans ce lieu est elle aussi justifiée. Toutefois, cette hypothèse *n'*est *pas* justifiée dans le cas des ordinateurs, étant donné que ceux-ci ne sont pas assimilables aux autres contenants susceptibles de se trouver dans le lieu perquisitionné. La nature particulière des ordinateurs commande une analyse distincte de la question de savoir si l'intrusion que représente la fouille d'un ordinateur est justifiée, auquel cas une autorisation préalable est nécessaire.

(i) Existence de différences entre les ordinateurs et les autres « contenants »

[40] Il est difficile d'imaginer une atteinte plus grave à la vie privée d'une personne que la fouille de son ordinateur personnel : *Morelli*, par. 105; *R. c. Cole*, 2012 CSC 53, [2012] 3 R.C.S. 34, par. 3.

"a multi-faceted instrumentality without precedent in our society": A. D. Gold, "Applying Section 8 in the Digital World: Seizures and Searches", prepared for the 7th Annual Six-Minute Criminal Defence Lawyer (June 9, 2007), at para. 3 (emphasis added). Consider some of the distinctions between computers and other receptacles.

[41] First, computers store immense amounts of information, some of which, in the case of personal computers, will touch the "biographical core of personal information" referred to by this Court in *R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293. The scale and variety of this material makes comparison with traditional storage receptacles unrealistic. We are told that, as of April 2009, the highest capacity commercial hard drives were capable of storing two terabytes of data. A single terabyte can hold roughly 1,000,000 books of 500 pages each, 1,000 hours of video, or 250,000 four-minute songs. Even an 80-gigabyte desktop drive can store the equivalent of 40 million pages of text: L. R. Robinton, "Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence" (2010), 12 *Yale J.L. & Tech.* 311, at pp. 321-22. In light of this massive storage capacity, the Ontario Court of Appeal was surely right to find that there is a significant distinction between the search of a computer and the search of a briefcase found in the same location. As the court put it, a computer "can be a repository for an almost unlimited universe of information": *R. v. Mohamad* (2004), 69 O.R. (3d) 481, at para. 43.

[42] Second, as the appellant and the intervener the Criminal Lawyers' Association (Ontario) point out, computers contain information that is automatically generated, often unbeknownst to the user. A computer is, as A. D. Gold put it, a "fastidious record keeper" (para. 6). Word-processing programs will often automatically generate temporary files that permit analysts to reconstruct the development

L'ordinateur constitue [TRADUCTION] « un instrument aux multiples facettes sans précédent dans notre société » : A. D. Gold, « Applying Section 8 in the Digital World : Seizures and Searches », document préparé pour le 7th Annual Six-Minute Criminal Defence Lawyer (9 juin 2007), par. 3 (je souligne). Considérons maintenant certaines des distinctions qui existent entre les ordinateurs et les autres contenants.

[41] Premièrement, les ordinateurs stockent d'immenses quantités de données, dont certaines, dans le cas des ordinateurs personnels, touchent à l'« ensemble de renseignements biographiques d'ordre personnel » qu'a mentionné notre Cour dans *R. c. Plant*, [1993] 3 R.C.S. 281, p. 293. L'ampleur et la variété de cette information rendent irréalistes les comparaisons avec les contenants traditionnels de stockage. On nous dit que, en avril 2009, les lecteurs de disque dur commerciaux dotés de la plus importante capacité de mémoire pouvaient stocker deux téraoctets de données. Or, un seul téraoctet peut contenir à peu près 1 000 000 de livres de 500 pages chacun, 1 000 heures de vidéo ou 250 000 chansons de quatre minutes. Même le disque dur de 80 gigaoctets d'un ordinateur de bureau peut stocker l'équivalent de 40 millions de pages de texte : L. R. Robinton, « Courting Chaos : Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence » (2010), 12 *Yale J.L. & Tech.* 311, p. 321-322. Compte tenu de cette capacité phénoménale de stockage, la Cour d'appel de l'Ontario a certainement eu raison de conclure qu'il existe une différence importante entre la fouille d'un ordinateur et celle d'une mallette trouvée au même endroit. Comme l'a exprimé la Cour d'appel, un ordinateur [TRADUCTION] « peut abriter un univers presque illimité d'informations » : *R. c. Mohamad* (2004), 69 O.R. (3d) 481, par. 43.

[42] Deuxièmement, comme le soulignent l'appelant et l'intervenante la Criminal Lawyers' Association (Ontario), les ordinateurs renferment des données qui sont générées automatiquement, souvent à l'insu de l'utilisateur. Comme l'a dit A. D. Gold, l'ordinateur [TRADUCTION] « tient les dossiers de façon très méticuleuse » (par. 6). En effet, il arrive souvent que les logiciels de traitement de texte

of a file and access information about who created and worked on it. Similarly, most browsers used to surf the Internet are programmed to automatically retain information about the websites the user has visited in recent weeks and the search terms that were employed to access those websites. Ordinarily, this information can help a user retrace his or her cybernetic steps. In the context of a criminal investigation, however, it can also enable investigators to access intimate details about a user's interests, habits, and identity, drawing on a record that the user created unwittingly: O. S. Kerr, "Searches and Seizures in a Digital World" (2005), 119 *Harv. L. Rev.* 531, at pp. 542-43. This kind of information has no analogue in the physical world in which other types of receptacles are found.

[43] Third, and related to this second point, a computer retains files and data even after users think that they have destroyed them. Oft-cited American scholar O. S. Kerr explains:

> . . . marking a file as "deleted" normally does not actually delete the file; operating systems do not "zero out" the zeros and ones associated with that file when it is marked for deletion. Rather, most operating systems merely go to the Master File Table and mark that particular file's clusters available for future use by other files. If the operating system does not reuse that cluster for another file by the time the computer is analyzed, the file marked for deletion will remain undisturbed. Even if another file is assigned to that cluster, a tremendous amount of data often can be recovered from the hard drive's "slack space," space within a cluster left temporarily unused. It can be accessed by an analyst just like any other file. [p. 542]

Computers thus compromise the ability of users to control the information that is available about them in two ways: they create information without the

génèrent automatiquement des fichiers temporaires permettant aux analystes de reconstituer l'élaboration d'un fichier et d'avoir accès à des renseignements indiquant qui a créé le fichier et qui y a travaillé. De même, la plupart des navigateurs utilisés pour consulter Internet sont programmés pour conserver automatiquement des renseignements concernant les sites Web que l'utilisateur a visités dans les semaines précédentes, ainsi que les syntagmes de recherche qu'il a utilisés pour y accéder. Normalement, ces renseignements peuvent aider l'utilisateur à retracer ses démarches cybernétiques. Dans le contexte d'une enquête criminelle, toutefois, ils peuvent également permettre aux enquêteurs d'avoir accès à des détails intimes concernant les intérêts, les habitudes et l'identité de l'utilisateur, à partir d'un dossier que ce dernier a créé sans le savoir : O. S. Kerr, « Searches and Seizures in a Digital World » (2005), 119 *Harv. L. Rev.* 531, p. 542-543. Les renseignements de ce genre ne possèdent pas d'équivalents dans le monde concret qui est celui des autres types de contenants.

[43] Troisièmement — et ce point est d'ailleurs lié au second —, l'ordinateur conserve des fichiers et des données même après que les utilisateurs croient les avoir détruits. Comme l'explique un auteur américain fréquemment cité, O. S. Kerr :

> [TRADUCTION] . . . le fait qu'un fichier ait été sélectionné et « supprimé » ne signifie pas normalement qu'il a effectivement été supprimé; les systèmes d'exploitation n'« éliminent » pas les zéros et les un associés à ce fichier lorsqu'il est sélectionné pour suppression. La plupart des systèmes d'exploitation modifient plutôt la table de fichiers principale pour indiquer que le bloc de mémoire de ce fichier est libre pour accueillir dans le futur d'autres fichiers. Si le système d'exploitation ne réutilise pas ce bloc pour un autre fichier au moment où l'ordinateur est analysé, le fichier qui a été sélectionné pour suppression reste en mémoire et peut être récupéré. Même si un autre fichier est inséré dans ce bloc de mémoire, une quantité phénoménale de données peut souvent être récupérée dans l'espace libre sur le disque dur, soit l'espace dans un bloc de mémoire temporairement non utilisé. Un analyste peut accéder à ce fichier comme à tout autre fichier. [p. 542]

Les ordinateurs compromettent ainsi de deux façons la capacité des personnes qui les utilisent de rester maîtres des renseignements disponibles à

users' knowledge and they retain information that users have tried to erase. These features make computers fundamentally different from the receptacles that search and seizure law has had to respond to in the past.

[44] Fourth, limiting the location of a search to "a building, receptacle or place" (s. 487(1) of the *Code*) is not a meaningful limitation with respect to computer searches. As I have discussed earlier, search warrants authorize the search for and seizure of things in "a building, receptacle or place" and "permit the search of receptacles such as filing cabinets, *within* that place . . . . The physical presence of the receptacle upon the premises permits the search": Fontana and Keeshan, at p. 1181 (italics in original; underlining added). Ordinarily, then, police will not have access to items that are not physically present in the building, receptacle or place for which a search has been authorized. While documents accessible in a filing cabinet are always at the same location as the filing cabinet, the same is not true of information that can be accessed through a computer. The intervener the Canadian Civil Liberties Association notes that, when connected to the Internet, computers serve as portals to an almost infinite amount of information that is shared between different users and is stored almost anywhere in the world. Similarly, a computer that is connected to a network will allow police to access information on other devices. Thus, a search of a computer connected to the Internet or a network gives access to information and documents that are not in any meaningful sense at the location for which the search is authorized.

[45] These numerous and striking differences between computers and traditional "receptacles" call for distinctive treatment under s. 8 of the *Charter*. The animating assumption of the traditional rule — that if the search of a place is justified, so is the

leur sujet : ils créent de l'information à l'insu des utilisateurs et ils conservent des données que ces derniers ont tenté d'effacer. En raison de ces caractéristiques, les ordinateurs sont fondamentalement différents des contenants que le droit relatif aux fouilles, perquisitions et saisies a dû régir par le passé.

[44] Quatrièmement, limiter l'endroit où la fouille se déroule à « un bâtiment, contenant ou lieu » (par. 487(1) du *Code*) ne constitue pas une restriction utile en ce qui concerne la fouille des ordinateurs. Comme je l'ai expliqué plus tôt, les mandats de perquisition autorisent les policiers à rechercher des choses dans « un bâtiment, contenant ou lieu » et à les saisir, et [TRADUCTION] « permettent de fouiller des contenants, tels des classeurs, *dans* le lieu perquisitionné [. . .] La présence physique du contenant sur les lieux permet d'effectuer une telle fouille » : Fontana et Keeshan, p. 1181 (italiques dans l'original; je souligne). Ordinairement, les policiers n'ont pas accès aux objets qui ne se trouvent pas physiquement dans le bâtiment, contenant ou lieu où la perquisition a été autorisée. Bien que les documents physiques auxquels on a accès dans un classeur se trouvent toujours au même endroit que le classeur lui-même, on ne peut en dire autant des renseignements auxquels on peut avoir accès au moyen d'un ordinateur. L'intervenante l'Association canadienne des libertés civiles souligne que les ordinateurs qui sont connectés à Internet servent de portails à une quantité presque infinie de données qui sont partagées entre différents utilisateurs et stockées presque n'importe où dans le monde. De même, un ordinateur connecté à un réseau permettra à la police d'avoir accès à des renseignements se trouvant dans d'autres appareils. Par conséquent, la fouille d'un ordinateur connecté à Internet ou à un réseau permet d'avoir accès à des données et à des documents qui ne se trouvent pas concrètement dans le lieu où la fouille est autorisée.

[45] Ces différences nombreuses et frappantes entre les ordinateurs et les « contenants » traditionnels commandent que ces objets soient traités différemment pour l'application de l'art. 8 de la *Charte*. L'hypothèse fondamentale à la base de la

search of receptacles found within it — simply cannot apply with respect to computer searches.

(ii) Prior Authorization Is Required

[46] Prior authorization of searches is a cornerstone of our search and seizure law. As the Court affirmed in *Hunter*, the purpose of s. 8 is "to protect individuals from unjustified state intrusions upon their privacy. That purpose requires a means of preventing unjustified searches before they happen . . . . This, in my view, can only be accomplished by a system of prior authorization" (p. 160 (emphasis in original)). Dickson J. went on in *Hunter* to say that the requirement of prior authorization "puts the onus on the state to demonstrate the superiority of its interest to that of the individual" (*ibid.*). The purpose of the prior authorization process is thus to balance the privacy interest of the individual against the interest of the state in investigating criminal activity *before* the state intrusion occurs.

[47] I have found that privacy interests in computers are different — markedly so — from privacy interests in other receptacles that are typically found in a place for which a search may be authorized. For this reason, I do not accept that a justice who has considered the privacy interests arising from the search of a place should be assumed to have properly considered the particular interests that could be compromised by a computer search. The distinctive privacy concerns that are at stake when a computer is searched must be considered in light of the purposes of s. 8 of the *Charter*. This calls for a specific assessment of "whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement": *Hunter*, at pp. 159-60. That is the threshold demanded by s. 8 of the *Charter*. Only a specific authorization to search a computer found

règle traditionnelle — à savoir que si la perquisition effectuée dans un lieu est justifiée, la fouille des contenants découverts dans ce lieu l'est également — ne peut tout simplement pas s'appliquer à la fouille des ordinateurs.

(ii) Nécessité de l'autorisation préalable

[46] L'autorisation préalable des perquisitions constitue une assise fondamentale de notre droit relatif aux fouilles, perquisitions et saisies. Comme l'a confirmé la Cour dans l'arrêt *Hunter*, l'art. 8 a pour but « de protéger les particuliers contre les intrusions injustifiées de l'État dans leur vie privée. Ce but requiert un moyen de prévenir les fouilles et les perquisitions injustifiées avant qu'elles ne se produisent [. . .] Cela ne peut se faire, à mon avis, que par un système d'autorisation préalable » (p. 160 (souligné dans l'original)). Le juge Dickson a ajouté, dans ce même arrêt, que l'exigence relative à l'autorisation préalable « impose à l'État l'obligation de démontrer la supériorité de son droit par rapport à celui du particulier » (*ibid.*). L'objectif du processus d'autorisation préalable est donc de mettre en balance le droit à la vie privée du particulier et l'intérêt de l'État à enquêter sur une activité criminelle, *avant* que l'intrusion de l'État ne se produise.

[47] J'ai conclu que les intérêts en matière de vie privée soulevés par les ordinateurs diffèrent — et ce nettement — de ceux que mettent en jeu d'autres contenants se trouvant habituellement dans les lieux où des perquisitions peuvent être autorisées. Pour cette raison, je ne peux admettre qu'il faille présumer qu'un juge de paix ayant considéré les intérêts en matière de vie privée que soulève la perquisition envisagée dans un lieu a dûment tenu compte des intérêts particuliers auxquels pourrait porter atteinte la fouille d'un ordinateur. Les préoccupations distinctives en matière de vie privée qui sont en jeu lors de la fouille d'un ordinateur doivent être examinées au regard des objectifs de l'art. 8 de la *Charte*. Il est donc nécessaire de se demander de façon particulière « si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment,

in the place of search ensures that the authorizing justice has considered the full range of the distinctive privacy concerns raised by computer searches and, having done so, has decided that this threshold has been reached in the circumstances of a particular proposed search.

[48] Specific, prior authorization means, in practical terms, that if police intend to search any computers found within a place they want to search, they must first satisfy the authorizing justice that they have reasonable grounds to believe that any computers they discover will contain the things they are looking for. They need not, however, establish that they have reasonable grounds to believe that computers will be found in the place, although they clearly should disclose this if it is the case. I would add here that once a warrant to search computers is obtained, police have the benefit of s. 487(2.1) and (2.2) of the *Code*, which allows them to search, reproduce, and print data that they find.

[49] If police come across a computer in the course of a search and their warrant does not provide specific authorization to search computers, they may seize the computer (assuming it may reasonably be thought to contain the sort of things that the warrant authorizes to be seized), and do what is necessary to ensure the integrity of the data. If they wish to search the data, however, they must obtain a separate warrant.

(iii) After-the-Fact Review Is Not Sufficient

[50] The Crown and intervening Attorneys General submit that specific, prior authorization to search computers is not necessary because an after-the-fact review of the manner in which a search is conducted provides sufficient protection for the

d'assurer l'application de la loi » : *Hunter*, p. 159-160. Voilà en quoi consiste le critère d'application de l'art. 8 de la *Charte*. Seul un mandat autorisant expressément la fouille des ordinateurs susceptibles d'être découverts dans le lieu perquisitionné garantit que le juge de paix qui a statué sur la demande d'autorisation a pris en compte l'ensemble des préoccupations distinctives en matière de vie privée que soulève la fouille de ces appareils, puis déterminé que ce critère était respecté eu égard aux circonstances de la fouille particulière projetée.

[48] Concrètement, une telle autorisation expresse préalable signifie que, si des policiers entendent fouiller tout ordinateur trouvé dans le lieu qu'ils souhaitent perquisitionner, ils doivent d'abord convaincre le juge de paix saisi de la demande d'autorisation qu'ils possèdent des motifs raisonnables de croire que les ordinateurs qu'ils pourraient découvrir contiendront les choses qu'ils recherchent. Les policiers ne sont toutefois pas tenus de démontrer qu'ils ont des motifs raisonnables de croire que des ordinateurs seront découverts dans le lieu concerné, mais ils devraient clairement dévoiler ce fait si c'est le cas. J'ajouterais ici que les policiers qui ont obtenu un mandat autorisant la fouille d'ordinateurs peuvent ensuite se prévaloir des par. 487(2.1) et (2.2) du *Code*, dispositions qui les autorisent à fouiller, à reproduire et à imprimer les données qu'ils trouvent.

[49] Si, durant une perquisition, les policiers trouvent un ordinateur et que leur mandat ne les autorise pas expressément à fouiller les ordinateurs, ils peuvent le saisir (pour autant qu'il soit raisonnable de croire que l'appareil contient le genre de choses que le mandat autorise à saisir) et prendre les mesures nécessaires pour assurer l'intégrité des données. Toutefois, s'ils désirent consulter ces données, ils doivent obtenir un mandat distinct.

(iii) Insuffisance du contrôle a posteriori

[50] Le ministère public et les procureurs généraux intervenants soutiennent que l'obtention d'une autorisation expresse préalable de fouiller des ordinateurs n'est pas nécessaire, parce que le contrôle a posteriori de la manière dont la fouille a

privacy rights that are at stake when a computer is searched. I disagree.

[51] As I explained above, if computers give rise to particular privacy interests that distinguish them from other receptacles typically found in a place, then s. 8 requires those interests to be taken into account *before* the search takes place, not just after-the-fact, in order to ensure that the state's interest in conducting the search justifies the intrusion into individual privacy. In effect, the privacy interests at stake when computers are searched require that those devices be treated, to a certain extent, as a separate place.

[52] As a result, I reject the Crown's submission that leaving the reasonableness of a computer search to after-the-fact review alone is compliant with the requirements of s. 8 of the *Charter*. As I explain next, however, I find the Crown's submissions to be more convincing with respect to the issue of whether authorizing justices should be constitutionally required to include search protocols in warrants authorizing the search of a computer.

(b) *A Warrant Authorizing the Search of Computers in the Circumstances of This Case Would Not Constitutionally Require the Imposition of Conditions Limiting How the Computers Were to Be Searched*

[53] The intervener the British Columbia Civil Liberties Association ("B.C.C.L.A.") submits that, in addition to a requirement that searches of computers be specifically authorized by a warrant, this Court should also find that these warrants must, as a rule, set out detailed conditions, sometimes called "*ex ante* conditions" or "search protocols", under which the search may be carried out. According to the B.C.C.L.A., search protocols are necessary because they allow authorizing justices to limit the way in which police carry out their

été effectuée protège suffisamment les droits en matière de vie privée que met en jeu la fouille d'un ordinateur. Je ne suis pas d'accord.

[51] Comme je l'ai expliqué précédemment, si les ordinateurs soulèvent des intérêts particuliers en matière de vie privée qui les distinguent des autres contenants habituellement trouvés dans un lieu, l'art. 8 commande alors que ces intérêts soient pris en compte *avant* l'exécution de la fouille — et non pas seulement après celle-ci — si l'on veut s'assurer que l'intérêt de l'État à effectuer la fouille justifie l'intrusion dans la vie privée de la personne concernée. En effet, en raison des intérêts en matière de vie privée que soulève la fouille d'un ordinateur, un tel appareil doit, dans une certaine mesure, être traité comme un lieu distinct.

[52] Par conséquent, je rejette l'argument du ministère public selon lequel le contrôle a posteriori du caractère non abusif de la fouille d'un ordinateur permet à lui seul d'assurer le respect des exigences de l'art. 8 de la *Charte*. Cependant, comme je vais l'expliquer ci-après, j'estime que les prétentions du ministère public sont plus convaincantes relativement à la question de savoir si les juges de paix saisis des demandes d'autorisation doivent être considérés comme tenus par la Constitution d'insérer des protocoles de perquisition dans les mandats autorisant la fouille d'ordinateurs.

b) *La Constitution n'exige pas qu'un mandat autorisant la fouille d'ordinateurs dans des circonstances comme celles qui nous occupent impose des conditions limitant la façon dont les ordinateurs doivent être fouillés*

[53] L'intervenante l'Association des libertés civiles de la Colombie-Britannique (« A.L.C.C.-B. ») soutient que, en plus d'exiger que la fouille des ordinateurs soit expressément autorisée par un mandat, notre Cour devrait également conclure qu'un tel mandat doit, en règle générale, énoncer des conditions détaillées — parfois appelées « conditions préalables » ou « protocoles de perquisition » — aux termes desquelles la perquisition peut être exécutée. Selon l'A.L.C.C.-B., les protocoles de perquisition sont nécessaires, parce qu'ils

searches, protecting certain areas of a computer from the eyes of the investigators. The Crown and intervening Attorneys General oppose this sort of requirement, arguing that it is contrary to principle and impractical. While I am not convinced that these sorts of special directions should be rejected as a matter of principle, my view is that they are not, as a general rule, constitutionally required and that they would not have been required in this case.

[54] While I propose, in effect, to treat computers in some respects as if they were a separate place of search necessitating distinct prior authorization, I am not convinced that s. 8 of the *Charter* requires, in addition, that the manner of searching a computer must always be spelled out in advance. That would be a considerable extension of the prior authorization requirement and one that in my view will not, in every case, be necessary to properly strike the balance between privacy and effective law enforcement. I reach this conclusion for two reasons.

[55] First, the manner of search is generally reviewed after the fact. That sort of detailed review with evidence and argument from both sides is better suited to developing new rules about how searches are to be conducted than is the *ex parte* procedure by which warrants are issued. *R. v. Boudreau-Fontaine*, 2010 QCCA 1108 (CanLII), is a good example of a case where the scope of a computer search was found to be unreasonable after the fact. The police had a search warrant authorizing them to examine a computer for evidence that the respondent had accessed the Internet. The Quebec Court of Appeal found that the police were not, by virtue of the warrant, authorized to scour the computer for evidence that the accused had engaged in the crime of distributing child pornography (para. 53). Thus, an *ex post* review of the reasonableness of a computer search in a particular case can signal to police how they should limit their

permettent au juge de paix saisi de la demande d'autorisation d'encadrer la façon dont les policiers effectuent leurs fouilles et de protéger ainsi certaines parties des ordinateurs du regard des enquêteurs. Pour leur part, le ministère public et les procureurs généraux intervenants s'opposent à une exigence de ce genre, plaidant qu'elle serait contraire aux principes pertinents et impossible à appliquer. Même si je ne suis pas convaincu que des directives spéciales de cette nature devraient par principe être écartées, je suis néanmoins d'avis que de telles directives ne sont pas, en règle générale, requises par la Constitution, et qu'elles n'auraient pas été nécessaires en l'espèce.

[54] Bien que je propose, dans les faits, de considérer qu'à certains égards un ordinateur constitue un lieu de fouille séparé nécessitant une autorisation préalable distincte, je ne suis pas persuadé que l'art. 8 de la *Charte* requiert en outre que la manière de fouiller un ordinateur soit toujours précisée à l'avance. Une telle condition aurait pour effet d'élargir considérablement l'obligation d'obtenir une autorisation préalable, et, à mon sens, elle ne serait pas nécessaire dans tous les cas pour établir un juste équilibre entre la protection de la vie privée et l'application efficace de la loi. J'arrive à cette conclusion pour deux raisons.

[55] Premièrement, la manière dont la perquisition a été exécutée fait généralement l'objet d'un contrôle a posteriori. Ce genre de contrôle minutieux, où les deux parties présentent des éléments de preuve et des arguments, est plus propice à l'élaboration de nouvelles règles sur la façon d'effectuer les fouilles que ne l'est la procédure *ex parte* de délivrance des mandats. L'arrêt *R. c. Boudreau-Fontaine*, 2010 QCCA 1108 (CanLII), constitue un bon exemple de situation où l'étendue de la fouille d'un ordinateur a, a posteriori, été jugée abusive. Les policiers étaient munis d'un mandat de perquisition les autorisant à fouiller un ordinateur afin d'y chercher des éléments de preuve indiquant que l'intimé avait accédé à Internet. La Cour d'appel du Québec a conclu que les policiers n'étaient pas autorisés par ce mandat à passer l'ordinateur au peigne fin à la recherche de preuves de la perpétration par l'accusé du crime

searches in future cases. Moreover, as has occurred in other areas of search law, after-the-fact review may lead courts to set out specific rules according to which searches must be conducted, as this Court did, for example, in *Descôteaux v. Mierzwinski*, [1982] 1 S.C.R. 860, at pp. 889-92.

de distribution de pornographie juvénile (par. 53). En conséquence, le contrôle a posteriori du caractère non abusif d'une fouille d'ordinateur dans un cas particulier peut indiquer aux policiers la façon dont ils devraient circonscrire leurs perquisitions dans de futures affaires. En outre, comme cela s'est produit dans d'autres domaines du droit en matière de perquisitions et de fouilles, le contrôle a posteriori peut amener les tribunaux à établir des règles précises sur la manière dont les fouilles et perquisitions doivent être effectuées, comme l'a fait notre Cour dans l'arrêt *Descôteaux c. Mierzwinski*, [1982] 1 R.C.S. 860, p. 889-892.

[56] Of course, developments in the case law may also spur parliamentary action aimed at tackling the issues more comprehensively. The *Criminal Code* contains certain rules which impose conditions, or require the authorizing justice to impose conditions, relating to the manner in which searches may be conducted. For example, s. 488 of the *Code* stipulates that a warrant (issued under s. 487 or s. 487.1) shall generally be executed by day. Also, the *Code* and this Court have set out special rules governing the manner of search — in effect, search protocols — in relation to documents for which solicitor-client privilege is claimed: s. 488.1; *Lavallee, Rackel & Heintz v. Canada (Attorney General)*, 2002 SCC 61, [2002] 3 S.C.R. 209, at para. 49. Similarly, s. 186(4)(*d*) requires a judge who issues an intercept authorization to impose such terms and conditions as are advisable in the public interest. I would not at this point foreclose similar developments with respect to computer searches as the law evolves through reviews of searches at trial and, if Parliament is so inclined, through legislative action.

[56] Il va de soi que l'évolution de la jurisprudence peut également inciter le législateur à intervenir en vue de régler certaines questions de façon plus globale. Le *Code criminel* comporte en effet certaines règles qui assujettissent l'exécution des fouilles au respect de certaines conditions ou qui obligent le juge de paix saisi de la demande d'autorisation à imposer des conditions. Par exemple, l'art. 488 du *Code* précise qu'un mandat (décerné en vertu de l'art. 487 ou 487.1) doit généralement être exécuté de jour. De plus, le *Code* et notre Cour ont énoncé des règles particulières régissant la manière d'effectuer les perquisitions — en fait, des protocoles de perquisition — dans le cas de documents à l'égard desquels le privilège des communications entre client et avocat est invoqué : art. 488.1; *Lavallee, Rackel & Heintz c. Canada (Procureur général)*, 2002 CSC 61, [2002] 3 R.C.S. 209, par. 49. De même, l'al. 186(4)*d*) oblige le juge qui accorde une autorisation d'intercepter des communications privées à imposer les modalités qu'il estime opportunes dans l'intérêt public. À ce stade-ci, je n'écarte pas la possibilité que les règles encadrant la fouille des ordinateurs connaissent des développements analogues, à mesure que le droit évolue par suite soit du contrôle des fouilles lors des procès, soit des interventions du législateur, lorsque celui-ci sent le besoin de le faire.

[57] Second, requiring search protocols to be imposed as a general rule in advance of the search would likely add significant complexity and practical difficulty at the authorization stage. At that point, an authorizing justice is unlikely to be able

[57] Deuxièmement, le fait d'exiger que soient en règle générale imposés des protocoles de perquisition avant l'exécution de la fouille rendrait vraisemblablement l'étape de l'autorisation beaucoup plus complexe, en plus de créer des difficultés d'ordre

to predict, in advance, the kinds of investigative techniques that police can and should employ in a given search or foresee the challenges that will present themselves once police begin their search. In particular, the ease with which individuals can hide documents on a computer will often make it difficult to predict where police will need to look to find the evidence they are searching for. For example, an authorizing justice's decision to limit a search for child pornography to image files may cause police to miss child pornography that is stored as a picture in a Word document. In short, attempts to impose search protocols during the authorization process risk creating blind spots in an investigation, undermining the legitimate goals of law enforcement that are recognized in the pre-authorization process. These problems are magnified by rapid and constant technological change.

pratique. En effet, à cette étape le juge de paix saisi de la demande d'autorisation n'est probablement pas capable de prédire le genre de techniques d'enquête que les policiers pourront et devront utiliser dans le cadre d'une perquisition donnée, ou encore de prévoir les défis qui surgiront une fois que les policiers commenceront leur perquisition. En particulier, vu la facilité avec laquelle les gens peuvent cacher des documents dans un ordinateur, il est souvent difficile de prédire l'endroit où les policiers devront fouiller pour trouver la preuve recherchée. Par exemple, si le juge de paix saisi de la demande d'autorisation dans une affaire de pornographie juvénile décide de limiter la perquisition aux fichiers images, les policiers pourraient passer à côté de photos pornographiques d'enfants insérées dans un document Word. Bref, les tentatives en vue d'imposer des protocoles de perquisition à l'étape de l'autorisation risquent de créer des angles morts dans une enquête et de contrecarrer les objectifs légitimes de l'application de la loi dont tient compte le processus d'autorisation préalable. Ces problèmes sont d'ailleurs amplifiés par l'évolution rapide et constante de la technologie.

[58] Courts in the United States have acknowledged the difficulty of predicting in advance where relevant files might be found on a computer. While the Tenth Circuit once suggested that police should be restricted to searching computers by file types, titles, or key words (see *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), at p. 1276), later cases have moved away from this approach: W. R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* (5th ed. 2012), vol. 2, at pp. 968-69. For example, in *United States v. Burgess*, 576 F.3d 1078 (10th Cir. 2009), decided 10 years after *Carey*, the same court held that "[i]t is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods . . . . [S]uch limits would unduly restrict legitimate search objectives" (pp. 1093-94). More recently, in *United States v. Christie*, 717 F.3d 1156 (10th Cir. 2013), the court found that "[c]omputer files can be misnamed by accident, disguised by intention, or hidden altogether, leaving investigators at a loss to know *ex ante* what sort of search will prove sufficient to ferret out the evidence they legitimately seek": p. 1166; see generally O. S. Kerr, "Ex Ante Regulation of

[58] Aux États-Unis, les tribunaux ont reconnu la difficulté de prédire où les dossiers pertinents peuvent se trouver dans un ordinateur. Bien que la Tenth Circuit Court ait déjà suggéré que les policiers ne devraient être autorisés à fouiller les ordinateurs que par types de fichier, par titres ou par mots clés (voir *United States c. Carey*, 172 F.3d 1268 (10th Cir. 1999), p. 1276), des décisions postérieures se sont éloignées de cette approche : W. R. LaFave, *Search and Seizure : A Treatise on the Fourth Amendment* (5e éd. 2012), vol. 2, p. 968-969. À titre d'exemple, dans *United States c. Burgess*, 576 F.3d 1078 (10th Cir. 2009), affaire décidée 10 ans après *Carey*, le même tribunal a tiré la conclusion qu'[TRADUCTION] « [i]l est irréaliste de s'attendre à ce qu'un mandat limite de façon prospective l'étendue d'une fouille par répertoires, noms de fichier ou extensions, ou tente de structurer des méthodes de fouille [. . .] [D]e telles limites restreindraient indûment les objectifs légitimes des fouilles » (p. 1093-1094). Plus récemment, dans *United States c. Christie*, 717 F.3d 1156 (10th Cir. 2013), la Tenth Circuit Court a conclu qu'[TRADUCTION] « [i]l peut arriver que des fichiers informatiques soient accidentellement mal désignés, intentionnellement camouflés ou

Computer Search and Seizure" (2010), 96 *Va. L. Rev.* 1241, at p. 1277.

[59] For these reasons, my view is that search protocols are not, as a general rule, constitutionally required for pre-authorization of computer searches. Nor, in my view, were they constitutionally required in this case.

[60] The computer searches here were aimed at evidence of ownership and occupation of a dwelling. There is nothing in the record that would assist us in formulating a practical and appropriate search protocol that could have been imposed in this case. Depending on how the computer was used, which police could not have known until they looked at the device, this evidence could have been found almost anywhere in the computer. For example, an address or image of the occupant could have been in a Word document, an Excel file, a tax-filing program, image or video files, various online accounts, etc. Moreover, a search of any one of these types of programs or files would not have assured access to the sought-after information. Finally, the police did not indicate any intention to use sophisticated forensic search methods to scour the device and they made no attempt to do so. In my view, there were no circumstances that pointed to a need for a search protocol to be included in a warrant authorizing the search of computers, should they be found in the residence.

[61] By now it should be clear that my finding that a search protocol was not constitutionally required in this case does not mean that once police had the warrant in hand, they had a licence to scour

encore tout simplement cachés, autant de situations qui empêchent les enquêteurs de savoir d'avance quel genre de fouille leur permettra de dénicher les preuves qu'ils recherchent légitimement » : p. 1166; voir, en général, O. S. Kerr, « Ex Ante Regulation of Computer Search and Seizure » (2010), 96 *Va. L. Rev.* 1241, p. 1277.

[59] Pour ces raisons, je suis d'avis que les protocoles de perquisition ne sont, en règle générale, pas requis par la Constitution en cas d'autorisation préalable de la fouille d'un ordinateur. De plus, aucun protocole de la sorte n'était constitutionnellement requis dans les circonstances de la présente affaire.

[60] En l'espèce, la fouille des ordinateurs visait des éléments de preuve confirmant l'identité des propriétaires et occupants d'une habitation. Il n'y a rien au dossier qui puisse nous aider à formuler un protocole de perquisition qui soit à la fois pratique et approprié, et qui aurait pu être imposé dans la présente affaire. Selon la façon dont les ordinateurs étaient utilisés — facteur que les policiers ne pouvaient connaître avant d'examiner les appareils — la preuve recherchée aurait pu être découverte à peu près n'importe où dans ceux-ci. Par exemple, l'adresse de l'occupant ou une photo de celui-ci aurait pu figurer dans un document Word, un fichier Excel, un logiciel de production de déclarations de revenus, des fichiers images ou vidéos, divers comptes en ligne, etc. En outre, la fouille de l'un ou l'autre de ces types de logiciels ou de fichiers n'aurait pas nécessairement permis de trouver l'information recherchée. Enfin, les policiers n'avaient d'aucune façon indiqué qu'ils entendaient recourir à des techniques d'investigation criminalistique perfectionnées pour passer l'appareil au peigne fin, et ils n'ont d'ailleurs fait aucune tentative de la sorte. À mon avis, aucune circonstance ne tendait à indiquer qu'il était nécessaire d'inclure un protocole de perquisition dans un mandat autorisant la fouille d'ordinateurs, au cas où de tels appareils seraient découverts dans la résidence.

[61] Il est sans doute évident, à ce point-ci, que ma conclusion selon laquelle aucun protocole de perquisition n'était requis par la Constitution en l'espèce ne signifie pas que, une fois munis d'un

the devices indiscriminately. They were bound, in their search, to adhere to the rule that the manner of the search must be reasonable. Thus, if, in the course of their search, the officers realized that there was in fact no reason to search a particular program or file on the device, the law of search and seizure would require them not to do so.

[62] Although I do not find that a search protocol was required on the particular facts of this case, authorizing justices must assure themselves that the warrants they issue fulfil the objectives of prior authorization as established in *Hunter*. They also have the discretion to impose conditions to ensure that they do. If, for example, an authorizing justice were faced with confidential intellectual property or potentially privileged information, he or she might find it necessary and practical to impose limits on the manner in which a computer could be searched. In some cases, authorizing justices may find it practical to impose conditions when police first request authorization to search. In others, they might prefer a two-stage approach where they would first issue a warrant authorizing the seizure of a computer and then have police return for an additional authorization to search the seized device. This second authorization might include directions concerning the manner of search. Moreover, I would not foreclose the possibility that our developing understanding of computer searches and changes in technology may make it appropriate to impose search protocols in a broader range of cases in the future. Without expressing any firm opinion on these points, it is conceivable that proceeding in this way may be appropriate in some circumstances.

mandat, les policiers étaient pour autant autorisés à passer sans discernement les appareils au peigne fin. En effet, ils demeuraient quand même tenus de se conformer à la règle requérant que la manière de procéder à la perquisition ne soit pas abusive. Par conséquent, s'ils s'étaient rendu compte durant la perquisition qu'il n'existait en fait aucune raison de fouiller un logiciel ou un fichier spécifique dans l'appareil, le droit relatif aux fouilles, perquisitions et saisies exigeait qu'ils s'abstiennent de le faire.

[62] Bien que j'estime qu'aucun protocole de perquisition n'était requis au vu des faits particuliers de la présente affaire, les juges de paix saisis d'une demande d'autorisation doivent s'assurer que les mandats qu'ils décernent répondent aux objectifs de la procédure d'autorisation préalable établis dans l'affaire *Hunter*. De plus, ils possèdent le pouvoir discrétionnaire d'imposer des conditions à cette fin. Si, par exemple, le juge de paix est en présence de renseignements concernant des droits de propriété intellectuelle confidentiels ou encore des renseignements susceptibles d'être protégés par un privilège, il pourrait décider qu'il est nécessaire et pratique d'imposer des limites quant à la manière dont un ordinateur peut être fouillé. Dans certains cas, le juge de paix peut estimer pratique d'imposer des conditions lorsque les policiers présentent leur demande d'autorisation de perquisitionner initiale. Dans d'autres circonstances, il pourrait préférer une démarche en deux temps, où il décernerait d'abord un mandat autorisant la saisie d'un ordinateur et exigerait que les policiers reviennent ensuite devant lui afin d'obtenir une autorisation supplémentaire leur permettant de fouiller l'appareil saisi. Cette seconde autorisation pourrait comporter des directives sur la manière de procéder à la fouille. En outre, je n'écarte pas la possibilité que l'amélioration de nos connaissances en matière de fouille d'ordinateurs ainsi que l'évolution des technologies puissent justifier, dans le futur, d'imposer des protocoles de perquisition dans un plus large éventail de situations. Je ne me prononce pas de façon ferme sur ces questions, mais il est par ailleurs concevable, selon moi, qu'une telle procédure puisse s'avérer appropriée dans certaines circonstances.

(c) *The Scope of These Reasons*

[63] It is not my intention to create a regime that applies to all computers or cellular telephones that police come across in their investigations, regardless of context. As the respondent correctly points out, police may discover computers in a range of situations and it will not always be appropriate to require specific, prior judicial authorization before they can search those devices. For example, I do not, by way of these reasons, intend to disturb the law that applies when a computer or cellular telephone is searched incident to arrest or where exigent circumstances justify a warrantless search. Rather, these reasons relate to those situations where a warrant is issued for the search of a place and police want to search a computer within that place that they reasonably believe will contain the things for which the search was authorized. As noted earlier, it is not necessary that the police present reasonable grounds that a computer will be found in order to obtain a warrant that includes authorization to search a computer found in the premises.

[64] While the scope of these reasons is restricted to warranted searches of a place, they apply equally to all computers found within a place with respect to which a search warrant has been issued. Put differently, any time that police intend to search the data stored on a computer found within a place for which a search has been authorized, they require specific authorization to do so. I find no reason, for the purposes of prior authorization, to treat computers differently on the basis of the particular use to which they have been put. For example, in this case, I make no distinction between the "personal" computer and the "security" computer for the purposes of prior authorization because both were capable of storing personal information. Computers do not distinguish between personal data and non-personal data; if information can be reduced to a series of ones and zeros, it can be stored on any computer. Moreover, decisions about whether or not to search the data

c) *Portée des présents motifs*

[63] Je n'ai pas l'intention de créer un régime applicable à tous les ordinateurs et téléphones cellulaires que trouvent les policiers au cours de leurs enquêtes, indépendamment du contexte. Comme le souligne à juste titre l'intimée, les policiers peuvent découvrir des ordinateurs dans des situations variées et il ne sera pas toujours indiqué d'exiger qu'ils obtiennent au préalable une autorisation judiciaire expresse avant de pouvoir fouiller les appareils. Par exemple, je n'entends pas, par les présents motifs, modifier le droit applicable lorsqu'un ordinateur ou un téléphone cellulaire est fouillé de façon incidente lors d'une arrestation, ou lorsque des circonstances pressantes justifient l'exécution d'une fouille sans mandat. Les présents motifs visent plutôt les situations où un mandat est décerné en vue d'autoriser une perquisition dans un lieu et où les policiers souhaitent pouvoir fouiller les ordinateurs qu'ils pourraient y trouver, parce qu'ils croient raisonnablement que ceux-ci contiendront les choses pour lesquelles la perquisition a été autorisée. Comme je l'ai souligné précédemment, il n'est pas nécessaire que les policiers qui désirent obtenir un mandat de perquisition autorisant aussi la fouille de tout ordinateur qui serait trouvé dans les lieux perquisitionnés présentent des motifs raisonnables de croire qu'un ordinateur sera découvert dans ceux-ci.

[64] Bien que la portée des présents motifs se limite aux perquisitions visant un lieu et autorisées par un mandat, les motifs s'appliquent également à tous les ordinateurs découverts dans le lieu à l'égard duquel un mandat de perquisition a été décerné. Autrement dit, chaque fois que les policiers ont l'intention de fouiller les données stockées dans un ordinateur découvert dans le lieu où une perquisition a été autorisée, ils ont besoin d'une autorisation expresse pour le faire. Je ne vois aucune raison, pour les besoins du processus d'autorisation préalable, de traiter les ordinateurs différemment les uns des autres selon l'utilisation particulière qui est faite de chacun. Par exemple, relativement à la délivrance de l'autorisation préalable, je ne fais aucune distinction en l'espèce entre l'ordinateur « personnel » et l'ordinateur de « sécurité », puisque les deux permettaient de stocker des renseignements personnels. Les ordinateurs ne distinguent pas les

on a device must be made before police know exactly what it contains. Rare will be the case where police know, at the authorization stage before they search a device, whether a computer is used for personal purposes or not. When it comes to authorization, then, I would treat all computers in the same way.

C. *Third Issue: Exclusion of the Evidence*

[65] In this case, the search warrant did not authorize the search of the computers found in the residence. As a result, the searches of those devices were not authorized by law and violated the appellant's right to be free of unreasonable search and seizure under s. 8 of the *Charter*. I must therefore address the question of whether the evidence found as a result of those searches was properly excluded at trial.

[66] The trial judge admitted the evidence obtained from the security computer but excluded the evidence derived from the search of the personal computer and the cellular telephone. The appellant is asking that the decision of the trial judge be restored and he does not contest her decision to admit the evidence from the security computer. My s. 24(2) *Charter* analysis is therefore limited to the evidence derived from the search of the personal computer and the cellular telephone.

[67] Although in general, a reviewing court should defer to a trial judge's s. 24(2) determination, I find I cannot do so in this case. In *R. v. Côté*, 2011 SCC 46, [2011] 3 S.C.R. 215, the majority of this Court found that "[w]here a trial judge has considered the proper factors and has not made any unreasonable finding, his or her determination is owed considerable deference on appellate review" (para. 44). However, where relevant factors have been overlooked or the trial judge has made an error, a fresh s. 24(2) analysis is necessary: *Cole*,

données qui sont personnelles de celles qui ne le sont pas; si des renseignements peuvent être réduits à une série de un et de zéros, ils peuvent être stockés dans n'importe quel ordinateur. Qui plus est, la décision de fouiller ou non les données se trouvant dans un appareil est nécessairement prise avant que les policiers sachent exactement ce que contient celui-ci. Il arrive rarement que les policiers sachent, à l'étape de l'autorisation précédant la fouille d'un ordinateur, si cet appareil est utilisé à des fins personnelles ou non. Par conséquent, pour ce qui concerne l'autorisation, je traiterais tous les ordinateurs de la même façon.

C. *Troisième question : exclusion de la preuve*

[65] En l'espèce, le mandat de perquisition n'autorisait pas la fouille des ordinateurs découverts dans la résidence. Par conséquent, la fouille de ces appareils n'était pas autorisée par la loi et violait le droit de l'appelant à la protection contre les fouilles, les perquisitions et les saisies abusives que lui garantit l'art. 8 de la *Charte*. Je dois donc décider si les éléments de preuve recueillis par suite de cette fouille ont à juste titre été écartés au procès.

[66] La juge de première instance a admis la preuve tirée de l'ordinateur de sécurité, mais écarté celle découlant de la fouille de l'ordinateur personnel et du téléphone cellulaire. L'appelant demande le rétablissement de la décision de la juge de première instance, mais ne conteste pas la décision de cette dernière d'admettre la preuve provenant de l'ordinateur de sécurité. En conséquence, mon analyse fondée sur le par. 24(2) de la *Charte* se limite à la preuve résultant de la fouille de l'ordinateur personnel et du téléphone cellulaire.

[67] Bien que, en règle générale, le tribunal siégeant en révision doive faire montre de déférence envers la décision rendue par le juge de première instance en vertu du par. 24(2), j'estime ne pas pouvoir le faire en l'espèce. Dans *R. c. Côté*, 2011 CSC 46, [2011] 3 R.C.S. 215, notre Cour a statué à la majorité que, « [l]orsque le juge du procès a pris en compte les considérations applicables et n'a tiré aucune conclusion déraisonnable, sa décision justifie une grande déférence en appel » (par. 44). Toutefois, lorsque des facteurs pertinents ont été

at para. 82. In her decision to exclude evidence in this case, the trial judge relied heavily on her finding that the ITO contained no facts supporting a warrant to search for documents evidencing ownership or occupation of the residence. For the reasons I set out in relation to the first issue on appeal, I conclude that this finding was erroneous. I must therefore undertake my own s. 24(2) analysis, of course accepting all of the trial judge's findings which are not tainted by any error.

[68] Section 24(2) of the *Charter* requires that evidence obtained in a manner that infringes the rights of an accused under the *Charter* be excluded from the trial if it is established that "having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute". The burden is on the party seeking exclusion to persuade the court that this is the case. In *R. v. Grant*, 2009 SCC 32, [2009] 2 S.C.R. 353, the Court established that

> [w]hen faced with an application for exclusion under s. 24(2), a court must assess and balance the effect of admitting the evidence on society's confidence in the justice system having regard to: (1) the seriousness of the *Charter*-infringing state conduct (admission may send the message the justice system condones serious state misconduct), (2) the impact of the breach on the *Charter*-protected interests of the accused (admission may send the message that individual rights count for little), and (3) society's interest in the adjudication of the case on its merits. [para. 71]

[69] Turning to the first factor, I conclude that the *Charter*-infringing state conduct was not serious. Although the trial judge characterized the conduct as "egregious", that conclusion is inextricably tied to her erroneous conclusion that the warrant did not authorize the search for documents relating to ownership and occupancy. When that finding is removed from the analysis, we are, in my view, left

négligés ou que le juge du procès a commis une erreur, une nouvelle analyse fondée sur le par. 24(2) s'impose : *Cole*, par. 82. La décision de la juge de première instance écartant des éléments de preuve en l'espèce repose considérablement sur sa conclusion que la Dénonciation ne faisait état d'aucun fait justifiant la délivrance d'un mandat de perquisition en vue de chercher des documents confirmant l'identité des propriétaires ou occupants de la résidence. Pour les motifs que j'ai énoncés au sujet de la première question soulevée par le présent pourvoi, j'estime que cette conclusion était erronée. En conséquence, je dois effectuer ma propre analyse fondée sur le par. 24(2), en faisant miennes, bien sûr, toutes les conclusions de la juge de première instance qui ne sont pas viciées par une erreur.

[68] Le paragraphe 24(2) de la *Charte* exige que les éléments de preuve obtenus d'une manière qui porte atteinte aux droits garantis à l'accusé par la *Charte* soient écartés du procès s'il est établi, « eu égard aux circonstances, que leur utilisation est susceptible de déconsidérer l'administration de la justice ». Il incombe à la partie qui sollicite l'exclusion des éléments de preuve de persuader le tribunal que c'est le cas. Dans l'arrêt *R. c. Grant*, 2009 CSC 32, [2009] 2 R.C.S. 353, la Cour a formulé l'analyse en ces termes :

> Ainsi, le tribunal saisi d'une demande d'exclusion fondée sur le par. 24(2) doit évaluer et mettre en balance l'effet que l'utilisation des éléments de preuve aurait sur la confiance de la société envers le système de justice en tenant compte de : (1) la gravité de la conduite attentatoire de l'État (l'utilisation peut donner à penser que le système de justice tolère l'inconduite grave de la part de l'État), (2) l'incidence de la violation sur les droits de l'accusé garantis par la *Charte* (l'utilisation peut donner à penser que les droits individuels ont peu de poids) et (3) l'intérêt de la société à ce que l'affaire soit jugée au fond. [par. 71]

[69] Pour ce qui est du premier facteur, je conclus que la conduite attentatoire de l'État n'était pas grave. Quoique la juge de première instance ait qualifié cette conduite d'[TRADUCTION] « indigne », cette conclusion est inextricablement liée à sa conclusion erronée selon laquelle le mandat n'autorisait pas la recherche de documents concernant l'identité des propriétaires et occupants.

with a search of a computer that was not expressly authorized by the search warrant but for which the police had reasonable grounds. It is also important, at this stage, to acknowledge that the ITO did refer to the intention of the officers to search for computer-generated documents and that the state of the law with respect to the search of a computer found inside premises was uncertain when police carried out their investigation. The Langley department had a policy of searching computers found on premises and there was no clear law prohibiting them from doing so. Indeed, the trial judge found that "the officers carried out the search in the belief that they were acting under the lawful authority of the warrant granted by the justice": *voir dire* decision, at para. 77. This case should serve to clarify the law on this point and prevent this kind of confusion in the future.

Une fois cette constatation écartée de l'analyse, il ne reste, à mon avis, qu'une fouille d'ordinateur qui n'était pas expressément autorisée par le mandat de perquisition, mais que les policiers avaient des motifs raisonnables d'exécuter. Il importe également, à cette étape-ci, de reconnaître que la Dénonciation faisait effectivement mention de l'intention des policiers de rechercher des documents générés par ordinateur et que l'état du droit relativement à la fouille d'ordinateurs découverts dans un lieu était incertain au moment où les policiers ont effectué leur enquête. Le service de police de Langley disposait d'une politique sur la fouille des ordinateurs trouvés sur les lieux d'une perquisition, et aucune règle de droit n'empêchait explicitement les policiers de se livrer à de telles fouilles. D'ailleurs, la juge de première instance a conclu que « les agents ont effectué la fouille en croyant agir sous l'autorité légitime du mandat décerné par le juge de paix » : décision sur le voir-dire, par. 77. La présente affaire devrait permettre de clarifier le droit sur cette question et de prévenir ce genre de confusion à l'avenir.

[70] That said, there are two somewhat disquieting aspects of the search of the computer. First, Sgt. Wilde admitted in his testimony that he intentionally did not take notes during the search so he would not have to testify about the details. This is clearly improper and cannot be condoned. Although I do not decide here that they are a constitutional prerequisite, notes of how a search is conducted should, in my view, be kept, absent unusual or exigent circumstances. Notes are particularly desirable when searches of computers are involved because police may not be able to recall the details of how they proceeded with the search. Second, I share the trial judge's concern that Sgt. Wilde obtained evidence by searching one of the seized computers after the detention order had expired. That search related to the security computer, however, and the evidence obtained as a result of that search is not in issue under s. 24(2), as I explained earlier.

[70] Cela dit, la fouille des ordinateurs en l'espèce présente toutefois deux aspects assez troublants. Premièrement, le sergent Wilde a admis dans son témoignage qu'il avait intentionnellement omis de prendre des notes durant cette fouille afin de ne pas avoir à témoigner sur les détails de celle-ci. Il s'agit là d'une conduite clairement répréhensible, qui ne saurait être tolérée. Bien que je ne décide pas, en l'espèce, que de telles notes sont requises sur le plan constitutionnel, les policiers devraient à mon avis prendre des notes sur la façon dont la fouille est effectuée, sauf en cas de situations pressantes ou inhabituelles. La prise de notes est particulièrement souhaitable lors de la fouille d'ordinateurs, étant donné que les policiers pourraient ne pas être en mesure de se rappeler en détail comment ils y ont procédé. Deuxièmement, tout comme la juge de première instance, je suis préoccupé par le fait que le sergent Wilde a obtenu des éléments de preuve en fouillant, après l'expiration de l'ordonnance de détention, l'un des ordinateurs qui avaient été saisis. Cette fouille visait toutefois l'ordinateur de sécurité, et la preuve ainsi recueillie n'est pas contestée en vertu du par. 24(2), comme je l'ai expliqué précédemment.

[71] Given the uncertainty in the law at the time and the otherwise reasonable manner in which the search was carried out, I conclude that the violation was not serious. The trial judge's opposite conclusion was clearly premised on her legal error respecting authorization to search for documents relating to ownership and occupation.

[72] I turn to the second stage of the inquiry. I accept the trial judge's finding that the privacy interests that are at stake in computer searches are of the highest order and that the search conducted here was "very intrusive and comprehensive": *voir dire* decision, at para. 83. At the same time, the record does not indicate that the police gained access to any more information than was appropriate, given the fairly modest objectives of the search as defined by the terms of the warrant. As the trial judge pointed out, the computers in this case were not forensically examined as they were in *Morelli*. On balance, this factor favours exclusion, but not strongly so.

[73] The third stage of the s. 24(2) inquiry requires the Court to consider society's interest in the adjudication of the case on its merits. The relevant question here is whether the truth-seeking function of the criminal trial process would be better served by admission of the evidence, or by its exclusion: *Grant*, at para. 79. The factors to be considered are the reliability of the evidence, the importance of the evidence to the Crown's case, and the seriousness of the offence, although this consideration has the potential to cut both ways: *Grant*, at paras. 81 and 83-84. The trial judge found that all the documents and photographs retrieved from the hard drives of the computers and the cellular telephone are reliable, real evidence. She also found that the evidence was required to establish knowledge of and control over the marijuana found growing in the basement of the residence. When the case was heard, the absence of this evidence substantially weakened the Crown's

[71] Comme le droit applicable était incertain au moment des faits pertinents et vu la manière par ailleurs non abusive dont la fouille a été effectuée, je conclus que la violation n'était pas grave. La conclusion contraire de la juge de première instance découlait manifestement de son erreur de droit concernant l'autorisation de rechercher des documents se rapportant à l'identité des propriétaires et occupants.

[72] Je passe maintenant à la deuxième étape de l'analyse. J'accepte la conclusion de la juge de première instance selon laquelle les intérêts en matière de vie privée que met en jeu la fouille d'un ordinateur sont extrêmement importants et que la fouille effectuée dans la présente affaire était [TRADUCTION] « très large et envahissante » : décision sur le voir-dire, par. 83. Par ailleurs, le dossier n'indique toutefois pas que les policiers ont eu accès à plus d'informations que ce qui était opportun, eu égard aux objectifs assez modestes de la fouille décrits dans le mandat. Comme l'a souligné la juge de première instance, en l'espèce les ordinateurs n'ont pas été fouillés par des experts comme l'avaient été ceux en cause dans l'affaire *Morelli*. Globalement, le présent facteur milite en faveur de l'exclusion, mais pas de façon déterminante.

[73] À la troisième étape de l'analyse fondée sur le par. 24(2), la Cour doit considérer l'intérêt de la société à ce que l'affaire soit jugée au fond. La question pertinente en l'espèce consiste à se demander si la fonction de recherche de la vérité que remplit le procès criminel serait mieux servie si on permettait l'utilisation de la preuve que si on l'écartait : *Grant*, par. 79. Les facteurs à prendre en compte sont la fiabilité des éléments de preuve, leur importance pour le ministère public et la gravité de l'infraction, quoique ce dernier facteur puisse jouer dans les deux sens : *Grant*, par. 81 et 83-84. La juge de première instance a conclu que l'ensemble des documents et des photos extraits des lecteurs de disque dur des ordinateurs et du téléphone cellulaire constituent des preuves matérielles fiables. Elle a également conclu que cette preuve était nécessaire pour établir la connaissance de l'existence de la marijuana cultivée dans le sous-sol de la résidence et le contrôle exercé sur celle-ci. Lorsque l'affaire

case. Finally, with respect to the third factor, I agree with the trial judge that there is a clear societal interest in adjudicating on their merits charges of production and possession of marijuana for the purpose of trafficking.

[74] Balancing these factors, I am of the view that the evidence should not be excluded. The police believed on reasonable grounds that the search of the computer was authorized by the warrant. While every search of a personal or home computer is a significant invasion of privacy, the search here did not step outside the purposes for which the warrant had been issued and it did not include forensic examination. The evidence obtained was reliable, real evidence which was important to the adjudication of the charges on their merits.

IV. Disposition

[75] I would dismiss the appeal and uphold the order of the Court of Appeal setting aside the acquittals entered after trial and directing a new trial.

Appeal dismissed.

Solicitors for the appellant: Cobb St. Pierre Lewis, Vancouver.

Solicitor for the respondent: Public Prosecution Service of Canada, Vancouver.

Solicitor for the intervener the Attorney General of Ontario: Attorney General of Ontario, Toronto.

Solicitor for the intervener the Attorney General of Alberta: Attorney General of Alberta, Calgary.

Solicitors for the intervener the British Columbia Civil Liberties Association: Ruby Shiller Chan Hasan, Toronto.

a été instruite, l'absence de ces éléments a considérablement affaibli la preuve du ministère public. Enfin, pour ce qui est du troisième facteur, tout comme la juge de première instance j'estime qu'il est manifestement dans l'intérêt de la société que des accusations de production et de possession de marijuana en vue d'en faire le trafic soient jugées au fond.

[74] Après avoir soupesé ces différents facteurs, je suis d'avis que les éléments de preuve ne doivent pas être écartés. Les policiers possédaient des motifs raisonnables de croire que la fouille des ordinateurs était autorisée par le mandat. Bien que toute fouille d'un ordinateur personnel constitue une atteinte importante à la vie privée, la fouille effectuée en l'espèce n'a pas débordé les objectifs pour lesquels le mandat avait été décerné et elle n'a pas donné lieu à une analyse criminalistique. Les éléments recueillis étaient des preuves matérielles fiables, qui étaient importantes pour permettre au tribunal de juger les accusations au fond.

IV. Dispositif

[75] Je rejetterais le pourvoi et je confirmerais l'ordonnance de la Cour d'appel annulant les acquittements inscrits à l'issue du procès et ordonnant la tenue d'un nouveau procès.

Pourvoi rejeté.

Procureurs de l'appelant : Cobb St. Pierre Lewis, Vancouver.

Procureur de l'intimée : Service des poursuites pénales du Canada, Vancouver.

Procureur de l'intervenant le procureur général de l'Ontario : Procureur général de l'Ontario, Toronto.

Procureur de l'intervenant le procureur général de l'Alberta : Procureur général de l'Alberta, Calgary.

Procureurs de l'intervenante l'Association des libertés civiles de la Colombie-Britannique : Ruby Shiller Chan Hasan, Toronto.

Solicitors for the intervener the Canadian Civil Liberties Association: Neuberger Rose, Toronto.

Solicitors for the intervener the Criminal Lawyers' Association (Ontario): Rosen Naster, Toronto.

Procureurs de l'intervenante l'Association canadienne des libertés civiles : Neuberger Rose, Toronto.

Procureurs de l'intervenante Criminal Lawyers' Association (Ontario) : Rosen Naster, Toronto.