SUPREME COURT OF CANADA

CITATION: R. *v*. Vu, 2013 SCC 60

DATE: 20131107
DOCKET: 34687

BETWEEN:

Thanh Long Vu
Appellant
and
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

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

REASONS FOR JUDGMENT: (paras. 1 to 75)
Cromwell J. (McLachlin C.J. and LeBel, Fish, Abella, Rothstein, Moldaver, Karakatsanis and Wagner JJ. concurring)

NOTE: This document is subject to editorial revision before its reproduction in final form in the *Canada Supreme Court Reports*.

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 phones — Whether search warrant properly permitting a search for documents evidencing ownership or occupation — Whether warrant authorized search of computers and cellular phone — If the search was unlawful, whether evidence obtained should be excluded — 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 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 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 phone. 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 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.

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); *Wilkerson v. State*, 594 A.2d 597 (1991); *R. v. Jones*, 2011 ONCA 632, 107 O.R. (3d) 241; *United States v. Carey*, 172 F.3d 1268 (1999); *United States v. Burgess*, 576 F.3d 1078 (2009); *United States v. Christie*, 2013 U.S. App. LEXIS 11704; *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; *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(1), (2.1), (2.2), 487.1, 488, 488.1.

Personal Information Protection and Electronic Documents Act, R.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 5th 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", 119 *Harv. L. Rev*. 531.

LaFave, Wayne R. *Search and Seizure: A Treatise on the Fourth Amendment*, 5th ed., vol. 4. 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.

Neil L. Cobb, *Elizabeth P. Lewis* 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 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 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.

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.

[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 phone?

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.

[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 hydrometer. 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.

[12] A Justice of the Peace issued a search warrant authorizing seizure of "[a]ll equipment and parts utilized to divert electricity, including 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 re-weighed the grounds set out in the ITO and substituted her view of the sufficiency of the evidence 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. (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.

[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 phone 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. 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.

[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.

[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.

[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 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 or *WordPerfect*. The search turned up the resume 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*, R.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 laptop computers, the cellular phone, 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 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 computers 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 laptops 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 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 phones were far more restricted than 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 cell phone 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 "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 point out, computers contain information that is automatically generated, often unbeknownst to the user. A computer is, as 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 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:

> [M]arking 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 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" 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" (s. 487(1)) and "permit the search of receptacles such as a filing cabinet, *within* that place . . . . The physical presence of the receptacle upon the premises permits the search": Fontana and Keeshan, at p. 1181 (italics in original; underling 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 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 v. Southam Inc.*, the purpose of s. 8 is "to protect individuals from unjustified state intrusion 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". 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 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.

(ii) 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 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 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 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 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.

[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 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.

[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 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.

[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 1076 (10th Cir. 2009), decided ten 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*, 2013 U.S. App. LEXIS 11704, 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. 15 (emphasis deleted); see generally O. S. Kerr, "Ex Ante Regulation of 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 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.

(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 phone 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 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 phone. 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 phone.

[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*, 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 *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 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.

[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 pre-requisite, 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.

[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, 83 and 84. The trial judge found that all the documents and photographs retrieved from the hard drives of the computers and the cellular phone 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 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.

Solicitors 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.

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

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