The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference

Volume 67 (2014) Article 13

Life after Vu: Manner of Computer Searches and Search Protocols

Gerald Chan

Life after *Vu*: Manner of Computer Searches and Search Protocols

Gerald Chan[*]

I. INTRODUCTION

Computers have been an indispensable part of our lives for at least two decades. Given the extent of our dependency on computers and the vast amounts of information that they contain, it was inevitable that they would become the focal point of criminal investigations. The only surprise is that it took so long for search and seizure law to join the party. Having repeatedly granted leave and issued sweeping judgments in this area in the past few years, the Supreme Court of Canada appears to be making up for lost time.

Police searches and seizures are primarily regulated by section 8 of the *Canadian Charter of Rights and Freedoms*. Section 8 guarantees everyone the right to be secure against unreasonable search and seizure,[1] and its purpose is to protect privacy.[2] To be considered reasonable, a search or seizure must: (i) be authorized by a law; (ii) that law must itself be reasonable; and (iii) the search or seizure must be carried out in a

---

[*] Partner at Ruby Shiller Chan Hasan, Barristers. The author wishes to thank Nader R. Hasan, with whom he has been co-counsel on a number of digital search and seizure cases and co-author of a number of papers on the same subject. The author's professional collaborations with Mr. Hasan have made an invaluable contribution to much of his own thinking in this challenging area of the law. The author also wishes to thank his law student, Jenn Aubrey, for her helpful feedback on an earlier draft of this paper.

[1] Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [hereinafter "Charter"].

[2] *Hunter v. Southam Inc. (sub nom. Canada (Combines Investigation Acts, Director of Investigation and Research) v. Southam Inc.)*, [1984] S.C.J. No. 36, [1984] 2 S.C.R. 145, at 159 (S.C.C.) [hereinafter "*Hunter v. Southam*"]. It should be noted, however, that the Supreme Court left open the possibility that the purpose of section 8 of the Charter is broader: "I would be wary of foreclosing the possibility that the right to be secure against unreasonable search and seizure must protect interests beyond the right of privacy, but for the purposes of the present appeal I am satisfied that its protections go at least that far."

reasonable manner.[3] The first two requirements can be further specified with reference to the Supreme Court's holding in *Hunter v. Southam*, which imposed a presumptive requirement that the search or seizure be pre-authorized by an impartial arbiter on the basis of reasonable and probable grounds to believe that a crime has been committed and that the search or seizure will reveal evidence of that crime.[4] Searches or seizures that do not satisfy this requirement of prior authorization are *prima facie* unreasonable.

Therefore, section 8 of the Charter will in most cases achieve its purpose of protecting privacy by imposing two prophylactic rules. First, the police must obtain prior authorization for the search or seizure, which will typically be in the form of a search warrant.[5] Second, even where a warrant has been issued, the search must be conducted in a reasonable manner.[6] The first rule prevents unjustified intrusions while the second rule regulates the extent of the intrusion.[7]

In three important cases, the Supreme Court of Canada applied these long-established, general principles of section 8 of the Charter to the digital world of computer searches. In *R. v. Morelli*, the Court wrote, that "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer"; and it is therefore important for the police to ensure that they have laid a proper basis for any warrant authorizing such a search.[8] Two years later in *R. v. Cole*, the Court held that the same principles apply to work computers, "at least where personal use is permitted or reasonably expected"; and the police must therefore obtain a warrant before searching the contents of such computers.[9] Just last year in *Vu*, the Court held that a warrant may only be relied on to search the contents of a

---

[3] *R. v. Collins*, [1987] S.C.J. No. 15, [1987] 1 S.C.R. 265, at 278 (S.C.C.) [hereinafter "*Collins*"].

[4] *Hunter v. Southam*, *supra*, note 2, at 160.

[5] *Id.*, at 160. There are exceptions to the requirement of prior authorization. For instance, the police may conduct a search of a person and his or her immediate surroundings incident to a lawful arrest: *R. v. Caslake*, [1998] S.C.J. No. 3, [1998] 1 S.C.R. 51, at para. 15 (S.C.C.). Whether and to what extent this exception applies to digital devices such as computers and cell phones will be determined by the Supreme Court of Canada in *R. v. Fearon*, [2013] S.C.C.A. No. 141 (S.C.C.) [hereinafter "*Fearon*"]. The case was heard on May 23, 2014 and is currently under reserve. The author was co-counsel to the British Columbia Civil Liberties Association in this case along with his partner, Nader R. Hasan.

[6] *Collins*, *supra*, note 3, at 278.

[7] *R. v. Vu*, [2013] S.C.J. No. 60, [2013] 3 S.C.R. 657, at para. 22 (S.C.C.) [hereinafter "*Vu*"].

[8] [2010] S.C.J. No. 8, [2010] 1 S.C.R. 253, at paras. 2-4 (S.C.C.) [hereinafter "*Morelli*"].

[9] [2012] S.C.J. No. 53, [2012] 3 S.C.R. 34, at para. 1 (S.C.C.) [hereinafter "*Cole*"].

computer where it specifically authorizes a computer search; a warrant that only authorizes the search of a residence in which a computer happens to be found is inadequate.[10]

These three cases provide useful guidance on the constitutional regulation of computer searches under section 8 of the Charter. Each of them, however, is concerned mainly with the first prophylactic rule requiring prior judicial authorization. This is, in many ways, the easier of the two rules. The question of whether and how the police should be required to obtain a warrant is relatively simple because it does not engage new processes. The police must decide whether the search of a particular computer (personal or work) engages a reasonable expectation of privacy; if it does, then the police must obtain a warrant before searching it. In order to do so, the investigating officer must swear an Information to Obtain setting out reasonable grounds to believe that a search of the computer will afford evidence of crime. The processes leading up to the obtaining of a warrant to search a computer are largely the same as they are for warrants to search other places and receptacles (*e.g.*, a house or car).

The second prophylactic rule governing the manner of search raises thornier problems when applied in the digital world. After decades of manner of search litigation, certain rules have emerged to govern searches and seizures in the physical world: for example, the police must ordinarily give notice before forcing entry; the police may use reasonable force to gain entry; and upon entry, the police are entitled to control the premises to ensure their safety and prevent the destruction of evidence. None of these rules, however, maps over easily to the digital world. There, the execution of a search warrant raises novel questions:

(1) Once the police have obtained a warrant to search a computer, can they look through every single file and folder in the computer?

(2) Are they limited to reviewing certain types of files?

(3) Should they be restricted to searching by certain keywords?

(4) What happens if they stumble upon evidence of one crime (*e.g.*, images of child pornography) in the course of searching for evidence of another crime (*e.g.*, documentation of fraud)?

---

[10] *Vu*, *supra*, note 7, at para. 3.

The Supreme Court of Canada has not yet had to grapple directly with any of these questions. But there is no doubt that these issues represent the next frontier of computer search and seizure law. In *Vu*, the Court invited counsel to engage in vigorous manner of search litigation in the computer context by emphasizing that a warrant to search a device does not give the police "a licence to scour the devic[e] indiscriminately".[11] Instead, if the police, in the course of their search, realize that there is no reason to search a particular program or file, the law of search and seizure would require them not to do so.[12] Moreover, the Court noted that while manner of search is generally reviewed after the fact,[13] issuing justices may find it "necessary and practical" to impose search protocols (*i.e.*, *ex ante* conditions) in certain cases.[14]

This paper seeks to build on these statements and imagine the post-*Vu* world of computer search and seizure law. Section 1 of Part II will summarize *Vu* and the propositions for which it stands. Section 2 will take up *Vu*'s invitation to carefully examine the manner of computer searches and draw on lower court decisions (in both Canada and the United States) in an attempt to tease out some general principles. Section 3 will analyze the issue of search protocols and when it might be appropriate — and, indeed, constitutionally required — for authorizing justices to impose *ex ante* conditions to regulate the manner of computer searches. The paper will conclude by urging the courts to adopt three general propositions to control the scope of computer searches so that they do not render the warrant requirement meaningless:

(1) The courts should carefully examine the methodology used by the police to determine whether they were faithful to the objectives of the warrant in their execution of the search.

(2) The courts should resist categorical claims that every file on a computer must be examined, even if only cursorily, to determine its relevance.

(3) The courts should require search protocols to be set out in the warrant in cases involving heightened privacy risks (*e.g.*, searches involving potentially privileged information and confidential intellectual property; searches aimed at networks of computers; and searches targeting innocent parties).

---

11 *Id.*, at para. 61.
12 *Id.*
13 *Id.*, at para. 55.
14 *Id*., at para. 62.

II. BEYOND A WARRANT REQUIREMENT: WHERE DO WE GO FROM *VU*?

1. *Vu*: What Did the Court Hold?

In *Vu*, 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. The warrant authorized the police to seize, among other things "documentation identifying ownership and/or occupancy of the property" relevant to an investigation of the offence.[15] It did not, however, specifically authorize the search or seizure of any computers or cell phones.

The police executed this warrant and discovered two computers and a cell phone in the residence. They searched these devices, and these searches led to evidence that Mr. Vu was the occupant of the residence.[16]

At trial, Mr. Vu claimed that these searches violated his rights under section 8 of the Charter and asked the judge to exclude the evidence. The trial judge found that police were not authorized to search the computers and cell phone because those devices were not specifically mentioned in the warrant. The trial judge excluded most of the evidence found as a result of these searches and acquitted the accused.[17]

The British Columbia Court of Appeal set aside the acquittal and ordered a new trial. It held that a computer is no different from "a four-drawer filing cabinet" when it comes to search and seizure law.[18] The general rule, with respect to physical objects, is that a warrant authorizing a search of a specific location for specific things authorizes the executing officers to conduct a reasonable examination of anything at that location within which the specified things might be found. "Just as it cannot be said that a warrant to search for documentary evidence relating to a fraudulent scheme would not apply to a four-drawer filing cabinet, the existence of which the police learn of after entering a residence," the Court of Appeal wrote, "neither can it be said that such a warrant would not apply to a computer, the existence of which the police learn of after entering a residence."[19]

---

15 *Id.*, at para. 12.
16 *Id*., at para. 4.
17 *R. v. Vu*, [2010] B.C.J. No. 1777, at paras. 60-69 (B.C.S.C.).
18 *R. v. Vu*, [2011] B.C.J. No. 2487, at para. 63 (B.C.C.A.).
19 *Id*., at para. 63.

The Supreme Court of Canada disagreed. In a unanimous judgment written by Cromwell J., the Court rejected the notion that a computer was no different from a physical container. "Computers differ in important ways from the receptacles governed by the traditional framework," Cromwell J. wrote, "and computer searches give rise to particular privacy concerns that are not sufficiently addressed by that approach."[20] Because computers raise unique privacy concerns, specific prior authorization must be obtained in order for a computer search to comply with section 8 of the Charter.

The Court delineated four important ways in which computers are different.

First, computers can "store immense amounts of information, some of which, in the case of personal computers, will touch the 'biographical core of personal information'".[21] An 80-gigabyte desktop drive — and commercial hard drives have far greater capacities — can store the equivalent of 40 million pages of text. Therefore, as the Ontario Court of Appeal put it in *R. v. Mohamad*, a computer "can be a repository for an almost unlimited universe of information".[22] This information touches on the most intimate aspects of our private lives.[23]

Second, a computer is, as Alan D. Gold has put it, a "fastidious record keeper".[24] Computers contain information that is automatically generated, often without the user knowing. Most web browsers, for instance, are programmed to automatically retain information about the websites that a user has visited in recent weeks in order to help the user retrace his or her cybernetic steps. This information can also, however, enable investigators to "access intimate details about a user's interests, habits, and identity, drawing on a record that the user has created unwittingly".[25]

Third, a computer retains files and data even after users think they have destroyed them.[26] When a user marks a file as deleted, the operating

---

[20] *Vu*, *supra*, note 7, at para. 2.

[21] *Id.*, at para. 41.

[22] [2004] O.J. No. 279, 69 O.R. (3d) 481, at para. 43 (Ont. C.A.), cited in *Vu*, *id.*, at para. 41.

[23] Orin Kerr, "Searches and Seizures in a Digital World (2005) 119 Harv. L. Rev. 531, at 569 [hereinafter "Kerr"]. See also *R. v. Morelli*, *supra*, note 8, at paras. 3, 105; *R. v. Cole*, *supra*, note 9, at para. 47; *R. v. Jones*, [2011] O.J. No. 4388, at para. 37 (Ont. C.A.) [hereinafter "*Jones*"].

[24] Alan 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.

[25] *Vu*, *supra*, note 7, at para. 42.

[26] *Id.*, at para. 43.

system simply goes to the "Master File Table" and marks 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 still be available for examination. Even if another file has been assigned to that cluster, a large amount of data can be recovered from the computer's "slack space", *i.e.*, space within the cluster left temporarily unused.[27] In this way, the computer's "delete" key is more aptly described as a "hide" key. Every inappropriate image, file or e-mail the user has ever viewed (even accidentally) will likely reside somewhere on the computer for years and be subject to examination by investigators no matter how quickly it was deleted.

Fourth, computers are rarely stand-alone, self-contained entities. 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".[28] Similarly, computers can be connected to networks or servers which link them to other computers.[29] This is often the case with computers found in a workplace. Consider, for instance, the single rogue trader in a multi-national financial firm who is suspected of engaging in insider trading from his workplace computer. A police officer with access to that employee's computer would be able to access the company's entire network, which might span five continents and contain the private files of hundreds of employees as well as sensitive information about the firm's clients.

These "numerous and striking differences" between computers and traditional receptacles, the Court held, call for "distinctive treatment under s. 8 of the *Charter*".[30] It is not enough for a warrant to authorize the search of a place in which a computer is found; the warrant must specifically authorize the search of a computer within that place. Only then, the Court held, can one be sure 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".[31]

---

27 *Id.*, at para. 43, citing Kerr, *supra*, note 23, at 542.
28 *Vu.*, *id.*, at para. 44.
29 *Id.*
30 *Id.*, at para. 45.
31 *Id.*, at para. 47.

The Court then went further and addressed a specific submission made by the intervener, British Columbia Civil Liberties Association (the "BCCLA").[32] The BCCLA had argued that it was not enough for a search warrant to simply include the word "computer"; rather, the unique privacy concerns raised by computers require police officers to submit, and justices to authorize, search protocols (*i.e.*, *ex ante* conditions) in advance of the search. These protocols would limit the scope of the computer search in order to ensure that, as much as possible, only that information which the police have reasonable grounds to search is in fact revealed.[33]

The Court did not accept this argument in its entirety, *i.e.*, it held that search protocols will not be constitutionally required in every case.[34] The manner of search, the Court held, is generally to be reviewed after the fact.[35] If the target of the search believes that police have exceeded the bounds of reasonableness in executing a search warrant on her computer, she may bring an application to seek Charter relief — and the reasonableness of the manner of search will then be determined on *ex post* review. Detailed rules governing the scope of the search generally do not need to be proposed by the police and spelled out in the warrant in advance of the search.

Importantly, however, the Court emphasized that the manner of search will be closely scrutinized on *ex post* review. Justice Cromwell wrote:

> 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 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.[36]

Moreover, the Court left the door open for search protocols to be imposed in certain cases. The Court noted that as the case law develops, "after-the-fact review may lead courts to set out specific rules according

---

[32] The author was co-counsel to the BCCLA in this case along with his partner, Nader R. Hasan.
[33] *Vu*, *supra*, note 7, at para. 53.
[34] *Id.*, at para. 54.
[35] *Id.*, at para. 55.
[36] *Id.*, at para. 61.

to which searches must be conducted", which can then be imported into search protocols.[37] In particular, the Court wrote that issuing justices may find it "necessary and practical" to impose search protocols in cases involving "confidential intellectual property or potentially privileged information".[38] In these cases, protocols could be imposed when police first request authorization to search the computer. Alternatively, issuing justices may prefer a "two-stage approach" where they would first issue a warrant authorizing the seizure of the computer and then have police return for an additional authorization to search the seized device, which would include a protocol that would limit the scope of the search.[39] Finally, the Court made it clear that it was not "foreclos[ing] 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".[40]

2. Manner of Search: How Will This Be Regulated?

The immediate lesson from *Vu* is that police officers must obtain a computer-specific warrant before searching the contents of any computers. But what does this mean beyond inserting the word "computer" in the warrant? The police must establish reasonable grounds to believe that a search of the computer will afford evidence of an offence before they can obtain a computer-specific warrant, but this will not be difficult to do in most cases. Given the ubiquity of computers and the immense amount and variety of information that they typically contain, the police should not have a hard time explaining why a computer will afford evidence of crime — especially if they already have reasonable grounds to believe that the place in which the computer is located contains evidence of crime.[41]

Beyond establishing the requisite grounds to search a computer and obtaining a warrant to do so, *Vu* makes it clear that most of the heavy lifting will be done on *ex post* review when the target challenges the

---

37 *Id.*, at para. 55.

38 *Id.*, at para. 62.

39 *Id.*

40 *Id.*

41 Lily 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 321 [hereinafter "Robinton"].

execution of the warrant under section 8 of the Charter. Only then will the manner in which the police searched the computer — *e.g.*, the number of files they looked at, when they looked at them and for how long — be measured against the standard for reasonableness under section 8.

In the physical world context, litigation over the manner of search has generated several rules for the police to follow. Before forcing entry, the police must ordinarily give: (i) notice of presence, by knocking or ringing the doorbell; (ii) notice of authority, by identifying themselves as law enforcement; and (iii) notice of purpose, by stating a lawful reason for entry.[42] The police may use reasonable force to gain entry.[43] Upon entry, the police are entitled to "control the premises" to ensure their safety and prevent the destruction of evidence.[44] Beyond controlling the premises, the police are not entitled to detain individuals simply because they happen to be found at the premises being searched, nor are they entitled to search their persons without some independent legal authority.[45]

These rules provide useful guidance for police officers and valuable protections for the privacy rights of individuals by, as much as possible, establishing bright lines beyond which the police must not go. The project of defining similar rules in the context of computer searches, however, is only beginning. Computers are different from ordinary places and receptacles and require a distinctive set of protections. Because of the four distinctive traits of computers explained in *Vu*, computer searches raise two unique challenges for manner of search regulation.

First, data are intermingled. Even where there are reasonable grounds to believe that a computer contains evidence of crime, there is a strong likelihood that the computer contains an "intermingling" of that evidence with intensely personal information that the police have no reasonable grounds to search or seize.[46] The same computer (or even the same folder

---

[42] *R. v. Cornell*, [2010] S.C.J. No. 31, [2010] 2 S.C.R. 142, at para. 43 (S.C.C.) [hereinafter "*Cornell*"].

[43] *R. v. Genest*, [1989] S.C.J. No. 5, [1989] 1 S.C.R. 59 (S.C.C.); *R. v. Gimson*, [1991] S.C.J. No. 104, [1991] 3 S.C.R. 692 (S.C.C.).

[44] *R. v. Silveira*, [1995] S.C.J. No. 38, [1995] 2 S.C.R. 297 (S.C.C.); *R. v. Strachan*, [1988] S.C.J. No. 94, [1988] 2 S.C.R. 980 (S.C.C.); *R. v. Learning*, [2010] O.J. No. 3092, at paras. 75-76 (Ont. S.C.J.).

[45] *Laporte v. Laganière J.S.P.*, [1972] Q.J. No. 3518, 29 D.L.R. (3d) 351 (Que. S.C.); *R. v. Thompson*, [1996] O.J. No. 1501 (Ont. Prov. Div.).

[46] See, *e.g.*, *Cole*, *supra*, note 9, at para. 88 (illegal photographs intermingled with photographs of the accused's wife); *In the Matter of the Search of 3817 W. West End*, 321 F.

within the computer) which contains fraudulent business records may also contain intimate medical records.

Second, the ordinary search and seizure process is inverted. In the physical world, physical realities limit the scope of the search. If, for example, the warrant authorizes the search and seizure of rifles, the police cannot reasonably search in a jewelry box. Computers, however, invert the process; the normal process of "search" and then selective "seizure" is turned on its head. Because of the difficulties of conducting an on-site search of computers, the police frequently seize computers without any prior review of their contents.[47] Police then take a mirror image of the entire hard drive so that they can search through its contents.[48] As a result, over-seizure is a particularly acute problem.[49] Computer searches involve "seiz[ing] the haystack to look for the needle".[50]

In light of these difficulties, how should the manner of a computer search be governed in order to strike the right balance between the interests of law enforcement and the privacy rights of individuals? While the jurisprudence is still in its infancy, some broad principles can be extracted from the lower court decisions in both the pre- and post-*Vu* eras; and some general observations can be made.

The Ontario Court of Appeal's decision in *Jones* is an important starting point. In that case, the police obtained a warrant to search the accused's home and computers for evidence of fraud. In the course of the computer search, the police discovered images of child pornography. The reviewing officer then conducted a full search of the hard drive,

---

Supp.2d 953, at 958 (N.D. Ill. 2004) [hereinafter "*West End*"]; *United States v. Otero*, 563 F.3d 1127, at 1132 (10th Cir. 2009).

47 *West End*, *id.*, at 958.

48 *Cole*, *supra*, note 9, at para. 5; *R. v. Little*, [2009] O.J. No. 3278, at para. 137 (Ont. S.C.J.) [hereinafter "*Little*"]; Kerr, *supra*, note 23, at 541. This has generally been found to be reasonable, although the courts have been careful not to foreclose the possibility that this technique may be unreasonable in a given case: *Little*, *id.*, at para. 164. See also See Christina M. Schuck, "A Search for the Caselaw to Support the Computer Search Guidance in *United States v. Comprehensive Drug Testing*" (2012) 16 Lewis & Clark L. Rev. 741, at 771 [hereinafter "Schuck"]. In *R. v. Cross*, [2007] O.J. No. 5384, at paras. 21-24 (Ont. S.C.J.), the Court held that imaging the hard drive was unreasonable because the warrant only authorized the police to search the computer for information concerning one e-mail. Similarly, in *R. v. Beitel*, [2011] O.J. No. 4331, at para. 29 (Ont. S.C.J.) [hereinafter "*Beitel*"], the Court held that imaging the hard drive was unreasonable because the computer contained sensitive and highly confidential information, such as the patient records of a psychiatrist.

49 *Jones*, *supra*, note 23, at para. 68.

50 *United States v. Hill*, 459 F.3d 966, at 975 (9th Cir. 2006).

including a search of video files that the officer would not have examined for the purposes of the fraud investigation.[51] The Court of Appeal held that this went beyond the scope of the warrant.

Writing for a unanimous panel, Blair J.A. dismissed the Crown's argument that a computer is an indivisible object that, once lawfully seized pursuant to a warrant, can be subject to a full examination of all data stored therein.[52] Instead, Blair J.A. adopted an *objective-based approach* for examining the manner of computer searches. "A computer search pursuant to a warrant," Blair J.A. wrote, "must be related to the legitimate targets respecting which the police have established reasonable and probable grounds, as articulated in the warrant."[53] That is, the reasonableness of the search depends on whether the police are confining themselves to the objective of the warrant, which in this case was to authorize a search for evidence of fraud (and not child pornography).

This approach can be contrasted with a *methodology-based approach*, in which the reasonableness of the search depends on whether the police are confining themselves to specific methods of searching a computer (*e.g.*, keyword searches, searching only document files and not videos, *etc.*).[54] Justice Blair rejected this approach as impractical:

> The focus on the type of evidence being sought, as opposed to the type of files that may be examined, is helpful, it seems to me, particularly in cases where it may be necessary for the police to do a wide-ranging inspection of the contents of the computer in order to ensure that evidence has not been concealed or its resting place in the bowels of the computer cleverly camouflaged.[55]

Justice Blair also considered the plain view doctrine and how it might apply in the computer search context. The plain view doctrine operates as an exception to the rule against warrantless seizures by allowing the police to seize evidence that falls outside the parameters of a warrant where: (i) the police are lawfully in the place where a search is being conducted; (ii) the incriminating nature of the evidence is immediately apparent; (iii) the evidence was discovered inadvertently; and (iv) no further

---

[51] *Jones*, *supra*, note 23, at paras. 8-11, 23-24.

[52] *Id.*, at paras. 45-46.

[53] *Id.*, at para. 42.

[54] See Stephen Guzzi, "Digital Searches and the Fourth Amendment: The Interplay Between the Plain View Doctrine and Search-Protocol Warrant Restrictions" (2012) 49 Am. Crim. L. Rev. 301.

[55] *Jones*, *supra*, note 23, at para. 43.

exploratory search is conducted to find evidence of other crimes.[56] Section 489 of the *Criminal Code* provides the police with a similar seizure power.[57]

Justice Blair applied the plain view doctrine to the facts of *Jones* and held that it permitted the officer to seize the images of child pornography that he initially encountered in his search of the computer for evidence of fraud. These images were inadvertently discovered in the course of a lawful search that was focused on the objective of the warrant. The plain view doctrine did not, however, allow the officer to then conduct a further exploratory search of the computer for evidence of child pornography.[58] This latter search was not inadvertent because the officer intentionally strayed from the objective of the warrant and embarked on a separate, unauthorized investigation. In this way, Blair J.A. reconciled the elements of the plain view doctrine with the objective-based approach to assessing reasonableness.

Jones made a useful contribution to the development of manner of search law in the computer context by setting out some general contours of reasonableness. In rejecting the Crown's "indivisible object" argument, *Jones* avoided an approach that would inevitably have led to a dramatic over-seizure in nearly every computer search case. In adopting an objective-based approach, *Jones* provided a framework within which the police can operate when conducting computer searches and a focal point for the courts when adjudicating the reasonableness of such searches.

It is important to note that while *Jones* rejects a methodology-based approach to determining reasonableness, the methodologies used by the police remain relevant insofar as they shed light on the subjective intent of the police in conducting the search. Three lower court decisions — each of which held that the manner of search was unreasonable — illustrate this point.

---

[56] *Id.*, at para. 56. See also *R. v. Spindloe*, [2001] S.J. No. 266, 154 C.C.C. (3d) 8, at 29-37 (Sask. C.A.); *R. v. F. (L.)*, [2002] O.J. No. 2604, at paras. 28-34 (Ont. C.A.); *R. v. Law*, [2002] S.C.J. No. 10, [2002] 1 S.C.R. 227, at para. 27 (S.C.C.).

[57] R.S.C. 1985, c. C-46. While some have suggested that section 489 is simply a codification of the plain view doctrine, the prevailing view in Ontario is that it is not: see *Jones*, *id.*, at para. 58; *R. v. B. (E.)*, [2011] O.J. No. 1042, at paras. 75-78 (Ont. C.A.), leave to appeal refused [2011] S.C.C.A. No. 455 (S.C.C.); *R. v. F. (L.)*, *id*., at para. 22. The key difference appears to be that the plain view exception requires the incriminating nature of the item seized to be "immediately apparent", while s. 489 requires only that the police have reasonable grounds to believe that the item will afford evidence of an offence. In *R. v. MacNeil*, [2014] B.C.J. No. 740, at para. 97 (B.C.S.C.), however, the Court articulated an important limitation on the s. 489 seizure power: it cannot be used to authorize the seizure of items deliberately excluded by the search warrant. See also s. 11(6) of the *Controlled Drugs and Substances Act*, S.C. 1996, c. 19.

[58] *Jones*, *id.*, at paras. 65-70.

In *Beitel*, the police claimed that they were conducting a stolen property investigation and searched the computer to determine its true ownership.[59] The investigating officer, however, testified that the first place he looked for ownership information was the recycling bin, where he restricted his search to picture files.[60] Further, the officer did not examine the serial number of the computer or conduct any other independent inquiries to ascertain ownership. Based on this evidence, the Court concluded that the officer "proceeded in the manner he did in order to see if the computer contained child pornography, not to determine lawful ownership of the computer".[61] The officer's methods were telling of his objective. The search was thus held to be unreasonable.

In *R. v. Perkins*, the police obtained a warrant to search a computer for "system files and logs" and "internet activity" in order to obtain evidence in relation to the offence of theft of telecommunications.[62] In executing the warrant, however, the reviewing officer began his search in the "lost files in the unallocated space, even though he knew that an easier source to find date and time of internet activity would be in the allocated space". (The unallocated space of a computer is where files are sent after the user has deleted them, but before the computer requires that space to store additional data.) Further, the reviewing officer did not "change the default settings of EnCase [*i.e.*, the forensic software he used to conduct the search] when he began his search, even though it is possible to a certain extent to limit the data scope and document scope of EnCase". The reviewing officer was "aware of tools such as a filter which allows for customized searches and a lock box which prevents graphic images from popping up", but he did not use these tools. Instead, he followed the same procedure as that which he typically used to search for child pornography. Again, the officer's methods were telling of his objective. The search was thus held to be unreasonable.[63]

In *R. v. Boudreau-Fontaine*, the police obtained a warrant to search the accused's computer for evidence proving that he had accessed the Internet, which he was prohibited from doing by probation order.[64] In the course of the computer search, the police discovered images of child pornography. The Quebec Court of Appeal held that the manner of search

---

59 *Beitel*, *supra*, note 48, at para. 25.
60 *Id.*, at para. 27.
61 *Id.*, at para. 31.
62 [2013] O.J. No. 1384, at para. 6 (Ont. S.C.J.).
63 *Id.*, at para. 106.
64 [2010] Q.J. No. 5399, at paras. 12, 47 (Que. C.A.).

was unreasonable: "the prosecution offered no evidence that would indicate whether the agents were still executing the warrant when they discovered the pornographic materials, that is, that they were still searching for information demonstrating that the computer had been connected to the Internet".[65] Implicit in this statement is the assumption that a police officer searching a computer for evidence of Internet access would be able to find such evidence long before stumbling upon images of child pornography.

These cases demonstrate that while the ultimate question in an objective-based approach concerns the subjective intent of the police, this intent can be inferred from the search methodology used by the police. More specifically, these cases suggest that the courts may effectively require the police to follow an "obvious to obscure" approach. As the U.S. Court of Appeals for the Tenth Circuit put it in *United States v. Burgess*, the officer must "first look in the most obvious places and as it becomes necessary to progressively move from the obvious to the obscure".[66] Failing to take such an approach may trigger an adverse inference that the police were in fact searching for evidence which falls outside the parameters of the warrant, *i.e.*, evidence of another crime.

Aside from articulating an objective-based approach to assessing reasonableness, *Jones* also contains some less helpful dicta about the permissible scope of computer searches. The most problematic dictum is the suggestion that the police may have to "examine any file or folder on the computer to reasonably accomplish [the] authorized search".[67] This statement was premised on the notion that electronic evidence may be "concealed" or "cleverly camouflaged" such that the only way to determine the true nature of files is to open and examine them, "at least

---

[65] *Id.*, at para. 53.

[66] 576 F.3d 1078, at 1094 (10th Cir. Wyo. 2009); Schuck, *supra*, note 48, at 779. The most recent example of the "obvious to obscure" approach can be found in *R. v. Sop*, [2014] O.J. No. 3666, 2014 ONSC 4610 (Ont. S.C.J.), which was released after this paper was submitted for publication. In that case, the police obtained a warrant on the basis of information that the accused had downloaded child pornography from a website, AZOV, between November 15 and December 15, 2010. But rather than beginning their search by looking for computer files with the word "AZOV" or computer files that were downloaded between November 15 and December 15, 2010, the police began their search by using EnCase to provide a gallery view of all of the images and videos on the device. They then engaged in "a systematic file by file search" (para. 149). The Court held that this was unreasonable. At para. 145, it wrote: "It is mildly troubling that the police would not have tried to search the computers using the two dates in question, the website, the hash values which were known and the Internet browser history or other techniques before doing what has been described as a very invasive general search."

[67] *Jones*, *supra*, note 23, at para. 44.

in a cursory fashion".[68] The police have made this assertion in a number of cases; it is inaccurate, but has frequently gone unchallenged.[69]

The police have the means to determine the true nature of files without opening and examining them. In *R. v. Sonne*, for instance, the evidence showed that the forensic software used by the police (*i.e.*, EnCase) was capable of determining whether the file type had been altered.[70] The same was true in *Ontario (Ministry of the Attorney General) v. Law Society of Upper Canada*.[71]

Indeed, many commentators have written about the ability of the police to conduct computer searches without opening files by searching based on "file headers" or "hash values". A "file header" is an internal computer file identifier that tells the computer about the file. Even if someone tries to disguise an image file by giving it a name and extension that makes it look like a word processing document, for example, the computer and forensic software will not be fooled because the file header will reveal the true nature of the file.[72] A "hash value" is a 32-character string of numbers and letters that serves as the "digital finger print" for the file. When the hash values of two files are the same, there is a sufficiently high statistical improbability of such a result occurring randomly that the two digital files are likely to be identical. The relationship between a hash value and its data set compares roughly to the relationship between an organism and its DNA sequence or fingerprint.[73]

Hash values are especially useful for the police when searching for images of child pornography. The police maintain an extensive database of the hash values of digital files previously deemed child pornography; and the police have access to similar databases maintained by other police forces, including those outside Canada. Thus, the police are able

---

[68] *Id.*, at para. 43.

[69] See also *R. v. Bishop*, [2007] O.J. No. 3806, at para. 47 (Ont. C.J.); *Little*, *supra*, note 48, at para. 93.

[70] [2012] O.J. No. 1200, 110 O.R. (3d) 209, at para. 66 (Ont. S.C.J.) [hereinafter " *Sonne*"].

[71] [2010] O.J. No. 2975, at para. 19 (Ont. S.C.J.) [hereinafter "*Law Society of Upper Canada*"]: "So far as can be guaranteed, the proposed process will put into police hands, for the purpose of investigation, only the images of child pornography and child nudity graphics and related material (e.g. chat lines, etc.) which the Examiner has, through the operation of sophisticated computer technology, classified and extracted from the images taken from the seized devices."

[72] See Schuck, *supra*, note 48, at 750.

[73] See *R. v. Braudy*, [2009] O.J. No. 347, at paras. 21-22 (Ont. S.C.J.); *R. v. Wonitowy*, [2010] S.J. No. 544, at para. 11 (Sask. Q.B.); Robinton, *supra*, note 41, at 326-27; Kerr, *supra*, note 23, at 544-46; Schuck, *supra*, note 48, at 777; Marc Palumbo, "How Safe is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment" (2010) XXXVI Fordham Urb. L.J. 97.

to search a computer for images of child pornography simply by searching the hash values of files in a computer and looking for matches with those in its databases.[74] They do not have to open each and every image file in the computer and can therefore avoid inadvertent exposure to all manner of private information such as intimate family photographs.[75] As one judge has said, new technologies may "give rise to new exigencies", but they also give rise to "new capabilities".[76]

This is not to say that searching by way of file headers and hash tags is foolproof — or that the police should always be limited to these forensic tools.[77] It is simply to suggest that the courts should be cautious about accepting the categorical claims of law enforcement that it will always be necessary to examine every file in the computer because the true nature of files may be concealed. Such claims are inaccurate because the police will often, although not always, have the technological tools to defeat such attempts at concealment. Moreover, such claims may be baseless where the target of the search is an innocent third party as opposed to a suspect. Even if such parties are able to conceal files, there is no reason to think that they will.[78]

If the police are always allowed to examine every file on a computer to determine its relevance, informational privacy will be obliterated. In *Little*, for example, the reviewing officer examined 13,000 files on the accused's computer to determine whether each of these files fell within the parameters of the warrant.[79] On most personal computers, this would include e-mails, Internet browsing history, instant messages, contacts, calendar appointments, photographs, videos, music audio files, and business, financial and medical records. The vast majority of these files would fall outside the parameters of the warrant; thus, the police would have had no grounds to review this information. To allow the police to

---

[74] *R. v. Braudy*, *id*., at para. 23; *R. v. Lamb*, [2010] B.C.J. No. 2701, at para. 17 (B.C.S.C.); *R. v. P. (O.)*, [2012] O.J. No. 2931, at para. 11 (Ont. S.C.J.); *R. v. Dominaux*, [2014] N.J. No. 16, at para. 9 (N.L. S.C.T.D.); *R. v. Johannson*, [2008] S.J. No. 827, at para. 6 (Sask. Q.B.); *R. v. Trapp*, [2011] S.J. No. 728, at para. 77 (Sask. C.A.); *R. v. Smith*, [2011] B.C.J. No. 437, at para. 34 (B.C.S.C.).

[75] See, *e.g*., *Cole*, *supra*, note 9, at para. 88.

[76] *United States of America v. Orphanou*, [2004] O.J. No. 622, at para. 62 (Ont. S.C.J.).

[77] Neither tool appears to be capable of determining whether one type of file has been hidden in another type of file (as opposed to the true nature of the file being altered). For instance, an image of child pornography could be embedded within a Word document. Searching by way of file headers would not raise any red flags because the true nature of the Word document would remain unchanged. See Robinton, *supra*, note 41, at 327; *Sonne*, *supra*, note 70, at para. 66.

[78] Schuck, *supra*, note 48, at 771.

[79] *Little*, *supra*, note 48, at para. 102.

access all of this information is to permit the police to sidestep the protections of section 8 of the Charter. This outcome is constitutionally intolerable.

In an attempt to offset the invasive nature of this search, the Court in *Little* added that while the officer's approach would be reasonable only if each file was "looked at cursorily to determine whether it [falls] within the parameters of the warrant"; in other words, the reviewing officer must immediately close any file that falls outside of these parameters.[80] There are at least three problems, however, with reliance on the cursory search standard to protect informational privacy.

First, as one commentator has noted, "if officers are allowed to cursorily examine the contents of each file in order to determine if a given document is within the scope of the warrant, an individual's protection depends upon police officers policing themselves".[81]

Second, even if one assumes that the police will always make a conscientious, good faith attempt to review each file no longer than absolutely necessary, the "cursory" search standard is unacceptably vague. The case law has, to date, been unable to provide any meaningful guidance as to where the line between cursory and non-cursory should be drawn. (In *Sonne*, for instance, all the Court could say is that the standard was met where the reviewing officer "flipped through" the files on the computer.[82]) And, this standard may well be eliminated when the Supreme Court of Canada considers it in the different context of searching a cell phone incident to arrest in *Fearon*.[83] Both the appellant and the respondent in *Fearon* have argued against the cursory search standard, calling it "impractical"[84] and "incapable of precise definition or consistent application".[85]

Third, the cursory search standard becomes meaningless if the plain view doctrine is applied in the computer search context as the Court of Appeal contemplated in *R. v. Jones*. If the police are entitled to review every single file — even if only cursorily — to determine whether it falls within the parameters of the warrant, then every such file will fall into

---

[80] *Id*., at para. 166.

[81] Schuck, *supra*, note, 48, at 778.

[82] *Sonne*, *supra*, note 70, at para. 67.

[83] *Supra*, note 5. This case was heard on May 23, 2014 and is currently under reserve.

[84] Appellant's Factum, para. 40 in *Fearon*, *id*., available online: <http://www.scc-csc.gc.ca/factums-memoires/35298/FM010_Appellant_Kevin-Fearon.pdf>.

[85] Respondent's Factum, para. 96 in *Fearon*, *id*., available online: <http://www.scc-csc.gc.ca/factums-memoires/35298/FM020_Respondent_Attorney-General-for-Ontario.pdf>.

"plain view" and be subject to seizure.[86] In other words, the police will always be in a lawful position from which to view (and seize) evidence of unrelated crimes and the warrant's scope would thus become meaningless.[87]

Accordingly, the courts should examine the facts of each case with great care — hopefully with the assistance of expert evidence and careful cross-examinations — to determine whether and when the police can legitimately claim that the danger of concealed files justifies the examination of every file on the computer. Such an approach should be the exception and not the rule. Just as the police cannot resort to the drastic measure of "dynamic entry" (*i.e.*, entering a residence with a battering ram) absent evidence of a possibility of violence,[88] the police should not be able to resort to the drastic measure of reviewing every file on a computer absent evidence of a file concealment that cannot otherwise be defeated.[89] Where the technological tools exist to allow the police to conduct a more surgical and less invasive search, they should be required to use them.

3. Search Protocols: When Will They Be Imposed?

The foregoing discussion is premised on the statement in *Vu* that manner of search is generally reviewed after the fact.[90] The Court did, however, hold out the possibility that issuing justices may find it "necessary and practical" to impose search protocols (*i.e.*, *ex ante* conditions) for computer searches in certain cases.[91] The Court also made it clear that it was not "foreclos[ing] the possibility that our developing understanding of computer searches and changes in technology may

---

[86] *Jones*, *supra*, note 23, at para. 62. See also Robinton, *supra*, note 41, at 330; RayMing Chang, "Why the Plain View Doctrine Should Not Apply to Digital Evidence" (2007) 12 Suffolk J. Trial & App. Advoc. 31, at 43-44; Kerr, *supra*, note 23, at 304-305; Samantha Trepel, "Digital Searches, General Warrants, and the Case for the Courts (2008) 10 Yale J.L. & Tech. 120, at 137-38.

[87] Robinton, *supra*, note 41, at 333. Many commentators have argued in favour of abolishing the plain view doctrine in the computer search context: see Kerr, *id.*, at 582-85; Chang, *id.*, at 59-61.

[88] *Cornell*, *supra*, note 42, at paras. 10, 20.

[89] It may be that the police should be required to return to the issuing justice for additional authorization to review every file on the computer if the police can show reasonable grounds to believe that such an invasive technique is necessary given the manner in which files are stored in the targeted computer, *e.g.*, where they have evidence that they are dealing with a sophisticated hacker.

[90] *Vu*, *supra*, note 7, at para. 55.

[91] *Id.*, at para. 62.

make it appropriate to impose search protocols in a broader range of cases in the future".[92]

In what sorts of cases can we expect to see search protocols imposed? And, how will they look when they are imposed? The Court gave two examples in *Vu*: cases involving "confidential intellectual property or potentially privileged information".[93] The latter provides a helpful starting point for an analysis of how search protocols should be designed.

Search protocols already exist for cases involving potentially privileged information — both for physical world searches and computer searches. In *Lavallee, Rackel & Heintz v. Canada (Attorney General)*,[94] the Supreme Court of Canada set out a number of rules to govern the legality of searches of law offices. These include:

(1) Before searching a law office, the investigative authorities must satisfy the issuing justice that there exists no other reasonable alternative to the search.

(2) Except when the warrant specifically authorizes the immediate examination, copying and seizure of an identified document, all documents in possession of a lawyer must be sealed before being examined or removed from the lawyer's possession.

(3) Every effort must be made to contact the lawyer and the client at the time of the execution of the search warrant.

(4) Where the lawyer or the client cannot be contacted, a representative of the Bar should be allowed to oversee the sealing and seizure of documents.

(5) If notification of potential privilege holders is not possible, the lawyer who had custody of the documents seized, or another lawyer appointed either by the Law Society or by the court, should examine the documents to determine whether a claim of privilege should be asserted, and should be given a reasonable opportunity to do so.[95]

---

92 *Id.*

93 *Id.*

94 [2002] S.C.J. No. 61, [2002] 3 S.C.R. 209 (S.C.C.).

95 *Id.*, at para. 49.

Following *Lavallee*, the Law Society of Upper Canada adopted a set of guidelines for lawyers to follow when their offices become the targets of search warrants.[96] These guidelines were recently implemented in the computer search context in *Law Society of Upper Canada*.[97] In that case, the police executed a search warrant for child pornography in an investigation against a criminal defence lawyer in Timmins, Ontario.[98] The Crown, the Law Society and the accused agreed on the following search protocol to protect solicitor-client privilege:

(1) An Examiner (*i.e.*, a forensic computer specialist) was to be appointed to conduct forensic procedures on the seized devices to enable the police and the Crown to obtain relevant evidence (the non-privileged graphic images of alleged child pornography).

(2) A Referee, a lawyer whose role is to assist the Court in ensuring that the procedure followed for searching the seized devices maximally protects solicitor-client privilege, was to be appointed.

(3) The Examiner was to create an EnCase forensic image of the physical drive from each original computer.

(4) The Examiner was to conduct further forensic searching of the EnCase images instead of working directly with the contents of the actual seized devices in order to preserve the integrity of the contents of the seized devices.

(5) The forensic investigation was to take place with the use of certain programs which "tease out" child pornography without the need to view privileged files: *e.g.*, the Examiner was to extract all digital files from each EnCase forensic image using C4P and C4M. The offensive material would be stored in an external storage device to be sealed pending a Crown application to unseal.

(6) The Examiner, with the assistance of the Referee, was to determine whether there were any privileged client files on the EnCase forensic images. If such privileged files were located, the Examiner was to

---

[96] Law Society of Upper Canada: Guidelines for Law Office Searches, online: <http://www.lsuc.on.ca/ guidelines-for-law-office-searches/>.

[97] *Supra*, note 71.

[98] *Id.*, at para. 2.

determine that no offensive materials were commingled among the privileged files and to copy the privileged files to a separate external storage device.

(7) The Examiner was to file with the Court a report chronicling his work.[99]

Among other things, this protocol is notable for the interposition of a neutral and detached third party between the investigating officers and the target of the warrant. Search protocols aimed at limiting search methodologies (*e.g.*, restricting the police to certain file types or keywords) have been criticized on the basis that a search "can be as much art as a science"[100] and that issuing justices "cannot get a sense of the exigencies that will unfold at each stage of the search process".[101] None of this criticism, however, impugns the interposition of a neutral and detached third party. The investigating officers can communicate the objectives of the warrant to the third party and then defer to the third party's judgment as to how best to pursue these objectives. So long as the third party has the necessary technical expertise, there will be no detriment to the investigation. There will, however, be an important advantage for informational privacy. Neutral and detached third parties are more likely to exercise restraint because they are not "engaged in the often competitive enterprise of ferreting out crime".[102] They are less likely to overlook important forensic tools that allow them to conduct less invasive and more surgical searches, and they have less incentive to engage in general exploratory searches of the computer's contents for evidence falling outside the parameters of the warrant.[103]

One expects that law enforcement will resist any requirement for a neutral and detached third party because it narrows their investigative discretion and can be costly. For the same reasons, the courts are unlikely to find that such an approach is constitutionally required in every computer search case. One can make a compelling argument, however, that this sort of search protocol should be required in an exceptional

---

[99] *Id.*, at para. 4 and Appendix A.

[100] *United States v. Brooks*, 427 F.3d 1246, at 1252 (10th Cir. Utah 2005).

[101] Orin Kerr, "Ex Ante Regulation of Computer Search and Seizure" (2010) 96 Va. L. Rev. 1241, at 1282.

[102] *Johnson v. United States*, 333 U.S. 10, at 14 (1948).

[103] In order for this to be a meaningful limitation on police power, the third party would have to be truly independent. The degree to which an ongoing business relationship with one party (*e.g.*, law enforcement) compromises the independence of experts will be considered by the Supreme Court of Canada in *White Burgess Langille Inman v. Abbott and Haliburton Co.*, [2013] S.C.C.A. No. 326 (S.C.C.), SCC File No. 35492, which is scheduled to be heard on October 7, 2014.

group of computer search cases in which privacy risks are heightened — whether because of the quantity or quality of information stored on the computers, or the extent of commingling between the incriminating evidence that the police expect to find and innocent but highly personal information that the police have no right to see. In addition to cases involving potentially privileged information, three categories of cases come to mind.

First, a neutral and detached third party may be required for searches involving *confidential intellectual property*. In *Vu*, the Supreme Court emphasized this as one category of information (along with potentially privileged information) that might require *ex ante* conditions to limit the scope of a computer search before it occurs.[104] Lower courts should build on this statement as the law develops.

Second, a neutral and detached third party may be required for searches involving *networks of computers*. As the Supreme Court noted in *Vu*, computers are rarely stand-alone, self-contained entities. They are often connected to networks or servers which link them to other computers.[105] The problem of intermingling and the consequential risk of over-seizure are exacerbated in this context.[106] In large companies, for instance, thousands of computers are connected to each other across cities, countries and continents via company network servers. These computer users share disk drives. If the police are allowed to search these networks without the oversight of a neutral third party, they could potentially comb through the private information of thousands of innocent people before they discover any evidence falling within the parameters of their warrant.

Consider the facts of *United States of America v. Equinix Inc.*[107] The United States was investigating Megaupload (a company that ran online file storage and viewing services) for criminal infringement of copyright, conspiracy to infringe copyright, money laundering and racketeering. To assist the United States with its investigation, the Attorney General of Canada seized 32 computer servers from Megaupload's Canadian office and applied for an order under section 15 of the *Mutual Legal Assistance in Criminal Matters Act*[108] to send mirror-imaged copies of all 32 servers

---

104 *Vu*, *supra*, note 7, at para. 62.

105 *Id.*

106 Schuck, *supra*, note 48, at 766.

107 [2013] O.J. No. 63 (Ont. S.C.J.) [hereinafter "*Equinix Inc.*"].

108 R.S.C. 1985, c. 30 (4th Supp.).

to the United States. The volume of data on these servers was the equivalent of that contained on 100 laptop computers. The Court found that "it is likely that the volume and breadth of data relevant to the prosecution as a whole is enormous".[109] Nevertheless, the Court declined to order all 32 servers to be sent to the United States; instead, it held that a more refined order was needed. The Court left it to the parties to decide how the scope of relevant material should be defined, subject to the matter being brought back to the Court if the parties could not agree.[110] The interposition of the Court in the process of identifying the information that the state should be allowed to review is analogous to a requirement for a neutral and detached third party to oversee the execution of a search warrant.

Third, a neutral and detached third party may be required for searches aimed at *innocent parties*.[111] Search warrants are not always obtained to search the computers of a suspect; they can also be obtained to search the computers of innocent parties, so long as there are reasonable grounds to believe that such computers contain evidence of crime. The best example of this may be *United States v. Comprehensive Drug Testing*.[112] There, the U.S. government conducted an investigation into the use of steroids by professional baseball players. The government obtained warrants to seize the drug-testing records of 10 named players from Comprehensive Drug Testing Inc. ("CDT"), a private company that administered anonymous drug testing services. In executing the warrant, however, the government seized the computers of the CDT and ended up reviewing the drug testing records of hundreds of players and many other people who had no connection to the investigation.[113] The state would not have been exposed to this highly personal information had the search been conducted by a neutral and detached third party.

The above examples focus on exceptional situations in which the privacy interests are even greater than they are in the ordinary computer search case — and, therefore, where the need for search protocols is enhanced. This, however, should not be taken to suggest that similar protocols should never be required when the police target

---

109 *Equinix Inc.*, *supra*, note 107, at para. 14.
110 *Id.*, at para. 16.
111 Schuck, *supra*, note 48, at 768.
112 579 F.3d 989 (9th Cir. 2009), revised 621 F.3d 1162 (9th Cir. 2010).
113 *Id.*, at 1166-67.

their search at a single computer. Indeed, there may be good reason to insist that such searches should always be conducted by an officer with special training in computer forensics and who is otherwise uninvolved in the investigation. Such an officer would not be a neutral and detached third party in the sense of being outside law enforcement, but he or she would at least be one step removed from the investigation. This procedure was followed in *R. v. Blazevic*, and it was upheld as reasonable under section 8 of the Charter on *ex post* review.[114]

III. CONCLUSION

The law of computer search and seizure is still in its infancy. The Supreme Court of Canada has answered some basic questions in *Morelli* (computer searches are invasive), *Cole* (warrants are required to search both personal and work computers) and *Vu* (warrants must specifically authorize a computer search). These decisions address the first prophylactic rule under section 8 of the Charter (*i.e.*, the requirement of prior authorization) in the computer search context. Now it is time to address the second rule that the manner of search must be reasonable — and this is where the hard work begins.

Developing manner of search law is challenging in the computer context because computer searches are driven by technology, which is constantly evolving. Thus, the imposition of overly specific rules enhances the risk of error. Such rules can unfairly limit the ability of the police to discover evidence that they have been authorized to seize, on the one hand, or overlook the ability of the police to conduct surgical searches that minimize the invasion of privacy, on the other hand.

This paper has attempted to focus on the general principles that can be extrapolated from the emerging case law and that can point the way forward while retaining the necessary flexibility to adapt to technological advances. These include the following propositions:

(1) The courts should carefully examine the methodology used by the police to determine whether they were faithful to the objectives of the warrant in their execution of the search.

---

[114] [2011] O.J. No. 6187, at paras. 13, 44 (Ont. S.C.J.).

(2) The courts should resist categorical claims that every file on a computer must be examined, even if only cursorily, to determine its relevance.

(3) The courts should require search protocols to be set out in the warrant in certain cases involving heightened privacy risks (*e.g.*, searches involving potentially privileged information and confidential intellectual property; searches aimed at networks of computers; and searches targeting innocent parties).

A proper balance between the interests of law enforcement and the privacy rights of individuals is critical in a free and democratic society. In the foreseeable future, this tension will manifest itself most significantly in computer searches. The Supreme Court of Canada has taken important steps to shore up the requirement of prior authorization in this context. The most important work, however, remains to be done. The courts must continue to focus on the many unique features of computers outlined in *Vu* as they develop new rules to regulate the manner of computer searches. Only this will ensure the continuing relevance of section 8 of the Charter in the digital age.