

IN THE SUPREME COURT OF CANADA  
(ON APPEAL FROM THE COURT OF APPEAL FOR BRITISH COLUMBIA)

BETWEEN:

THANH LONG VU

Appellant

- AND -

HER MAJESTY THE QUEEN

Respondent

- AND -

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION,  
CANADIAN CIVIL LIBERTIES ASSOCIATION,  
CRIMINAL LAWYERS' ASSOCIATION (ONTARIO),  
ATTORNEY GENERAL OF ALBERTA, and  
ATTORNEY GENERAL OF ONTARIO

Interveners

---

**FACTUM OF THE INTERVENER**  
**BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION**  
(Pursuant to Rules 37 and 42 of the *Rules of the Supreme Court of Canada*)

---

**RUBY SHILLER CHAN HASAN**

Barristers  
11 Prince Arthur Avenue  
Toronto, ON M5R 1B2

**Nader R. Hasan**

**Gerald J. Chan**  
Tel: (416) 964-9664  
Fax: (416) 964-8305

**Counsel for the Intervener,  
British Columbia Civil Liberties Association**

**SACK GOLDBLATT MITCHELL LLP**

Barristers and Solicitors  
500 – 30 Metcalfe Street  
Ottawa ON K1P 1C3

**Raija Pulkkinen**

Tel: (613) 235-5327  
Fax: (613) 235-3041

**Ottawa Agent for the Intervener,  
British Columbia Civil Liberties Association**

**ORIGINAL TO:**

**The Registrar**  
301 Wellington Street  
Ottawa, ON K1A 0J1

**COPIES TO:**

**COBB ST-PIERRE LEWIS**

#308 – 425 Carrall St.  
Vancouver, BC V6B 6E3

**Neil L. Cobb**  
**Elizabeth P. Lewis**  
**Nancy Seto**  
Tel: (604) 602-9770  
Fax: (604) 684-9690

**Counsel for the Appellant**

**PUBLIC PROSECUTION SERVICE OF  
CANADA**

900 – 840 Howe St.  
Vancouver, BC V6Z 2S9

**W. Paul Riley**  
**Martha M. Devlin, Q.C.**  
Tel: (604) 666-0704  
Fax: (604) 666-1599

**Counsel for the Respondent**

**NEUBERGER ROSE LLP**

1392 Eglinton Ave. W.  
Toronto, ON M6C 2E4

**David S. Rose**  
Tel: (416) 363-0761  
Fax: (416) 364-3271

**Counsel for the Intervener,  
Canadian Civil Liberties Association**

**GOWLING LAFLEUR HENDERSON LLP**

2600 – 160 Elgin St.  
Box 466 Station D  
Ottawa, ON K1P 1C3

**Brian A. Crane, Q.C.**

Tel: (613) 233-1781  
Fax: (613) 563-9869

**Agent for the Appellant**

**DIRECTOR OF PUBLIC PROSECUTION  
OF CANADA**

284 Wellington St.  
2<sup>nd</sup> Floor  
Ottawa, ON K1A 0H8

**François Lacasse**

Tel: (613) 957-4770  
Fax: (613) 941-7865

**Agent for the Respondent**

**GOWLING LAFLEUR HENDERSON LLP**

2600 - 160 Elgin St.  
Box 466 Station D  
Ottawa, ON K1P 1C3

**Brian A. Crane, Q.C.**  
Tel: (613) 233-1781  
Fax: (613) 563-9869

**Agent for the Intervener,  
Canadian Civil Liberties Association**

**ROSEN NASTER LLP**  
330 University Ave.  
Suite 504  
Toronto, ON M4G 1R7

**John M. Rosen**  
**Paul J.I. Alexander**  
Tel: (416) 927-9000  
Fax: (416) 927-9069

**Counsel for the Intervener,  
Criminal Lawyers' Association**

**ATTORNEY GENERAL OF ONTARIO**  
Crown Law Office Criminal  
720 Bay Street  
10th Floor  
Toronto, ON M5G 2K

**Michal Fairburn**  
Tel: (416) 326-4658  
Fax: (416) 326-4656

**Counsel for the Intervener,  
Attorney General of Ontario**

**ATTORNEY GENERAL OF ALBERTA**  
3rd Floor  
Centrium Place  
300, 332 – 6 Ave. S.W.  
Calgary, AB T2P 0B2

**Jolaine Antonio**  
Tel: (403) 592-4902  
Fax: (403) 297-3453

**Counsel for the Intervener,  
Attorney General of Alberta**

**GOWLING LAFLEUR HENDERSON LLP**  
2600 - 160 Elgin St.  
Box 466 Station D  
Ottawa, ON K1P 1C3

**Henry S. Brown, Q.C.**  
Tel: (613) 233-1781  
Fax: (613) 788-3433

**Agent for the Intervener,  
Criminal Lawyers' Association**

**BURKE-ROBERTSON**  
441 MacLaren St.  
Suite 200  
Ottawa, ON K2P 2H3

**Robert E. Houston, Q.C.**  
Tel: (613) 566-2058  
Fax: (613) 235-4430

**Agent for the Intervener,  
Attorney General of Ontario**

**GOWLING LAFLEUR HENDERSON LLP**  
2600 - 160 Elgin St.  
Box 466 Station D  
Ottawa, ON K1P 1C3

**Brian A. Crane Q.C.**  
Tel: (613) 233-1781  
Fax: (613) 563-9869

**Agent for the Intervener,  
Attorney General of Alberta**

## TABLE OF CONTENTS

PART I: STATEMENT OF FACTS	1
PART II: THE BCCLA’S POSITION ON THE QUESTION IN ISSUE	1
PART III: STATEMENT OF ARGUMENT	1
I. <i>Ex Ante</i> Search Protocols Are Necessary To Satisfy Section 8	1
A.    Benefits of Search Protocols	1
B.    Types of Search Protocols	3
C.    Authority for Search Protocols	5
D.    The Criticism of <i>Ex Ante</i> Search Protocols Is Unavailing	7
II.    Computer Searches Should Require “Investigative Necessity”	8
PART IV: SUBMISSIONS ON COSTS	10
PART V: NATURE OF THE ORDER REQUESTED	10
PART VI: TABLE OF AUTHORITIES	11

## PART I: STATEMENT OF FACTS

1. The British Columbia Civil Liberties Association (the “BCCLA”) accepts the facts as set out in the parties’ facts. The BCCLA takes no position on disputed facts.

## PART II: THE BCCLA’S POSITION ON THE QUESTION IN ISSUE

2. We live in a digital age. Yet, our s. 8 *Charter* jurisprudence on computer searches remains ossified in the pre-digital era. A computer is neither a filing cabinet nor a briefcase. Both individual privacy and law enforcement interests are best served if the courts adopt an approach to computer searches that reflects an understanding of modern technology.

3. The issue in this case is whether a search warrant must *specifically* authorize the search of a computer or whether a conventional warrant to search a dwelling *implicitly* authorizes a search of all computers therein. The BCCLA respectfully submits that a computer-specific search warrant is necessary because computer searches are different. They should therefore be subject to different rules. Section 8 of the *Charter* should require two prerequisites to be established before a computer warrant will issue: (i) prior judicial approval of computer search protocols; and (ii) investigative necessity. Both requirements follow from this Court’s recognition in *Morelli* that “it is difficult to imagine a more intrusive invasion of privacy than the search of one’s home and personal computer.”<sup>1</sup>

## PART III: STATEMENT OF ARGUMENT

### I. *EX ANTE* SEARCH PROTOCOLS ARE NECESSARY TO SATISFY SECTION 8

4. In order for a warrant to satisfy s. 8 of the *Charter*, it must be accompanied by a set of “search protocols.” By “search protocols”, the BCCLA refers to *ex ante* rules, proposed by the police and approved by the issuing justice, that specify how the police will conduct the computer search in a manner that satisfies the reasonableness requirement of s. 8 of the *Charter*. Depending on the case, the search protocols may limit the time, place or manner of the search. The protocols may also specify forensic tools and techniques to be used to minimize the intrusion into individual privacy and/or designate specially trained officers to conduct the search.

#### A. Benefits of Search Protocols

5. There are several reasons why search protocols should be required under s. 8 of the *Charter*.

---

<sup>1</sup> *R. v. Morelli*, [2010] 1 S.C.R. 253 at paras. 2, 105.

6. ***The Nature and Quantity of the Information.*** Both the quantity and quality of the information stored on computers weigh in favour of search protocols. While computers are physically compact, the amount of data that can be stored on a computer is staggering. A few years ago, for as little as \$150, anyone could purchase a computer hard drive with storage capacity of 500 gigabytes, which is roughly equivalent to 250 million pages of text — or about the amount of information contained in all of the books on six floors of an academic library.<sup>2</sup> Now, readily available external hard drives have several times that capacity for the same price. Without protocols, there is an omnipresent danger that computer searches will become unchecked fishing expeditions.<sup>3</sup>

7. This is especially dangerous in light of quality of information that is contained in computers. As noted in *Morelli* and *Cole*, virtually every aspect of one's private life is consolidated into one's computer, including "our most intimate correspondence", "details of our financial, medical, and personal situations", and "our specific interests, likes, and propensities" as revealed through the records of what we "seek out and read, watch, or listen to on the Internet."<sup>4</sup> People today use computers as photo albums, stereos, telephones, desktops, file cabinets, waste paper baskets, televisions, postal services, playgrounds, jukeboxes, dating services, movie theaters, shopping malls, personal secretaries, virtual diaries, and more.<sup>5</sup> And all of these uses create a permanent (or near-permanent) record on the computer's hard drive.<sup>6</sup> Therefore, the type of information found on computers "falls at the very heart of the 'biographical core' protected by s. 8 of the *Charter*."<sup>7</sup> Section 8 of the *Charter* should require the police and the issuing justice to turn their mind to the question of how the search can be appropriately tailored to minimize the invasion of privacy.

8. ***Intermingling of Data.*** Even where there are reasonable grounds to believe that a computer contains documents evidencing crime, there is a strong likelihood that this computer contains an

<sup>2</sup> "Hard Drives," online: PC Mag.com <<http://www.pcmag.com/reviews/hard-drives>>; Orin S. Kerr, "Searches and Seizures in a Digital World" (2006) 119 Harv. L. Rev. 531 at 542; see also Marc Palumbo, "How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment" (2009) 36 Fordham Urb. L.J. 977 at 995.

<sup>3</sup> See *United States v. Comprehensive Drug Testing Inc.*, 621 F3d 1162 at 1176-77 (9th Cir. 2010) (en banc), *modifying* 579 F.3d 989 (9th Cir. 2009) (en banc).

<sup>4</sup> *R. v. Morelli*, *supra* at paras. 3, 105 (S.C.C.); *R. v. Cole*, [2012] S.C.J. No. 53 at para. 47 (S.C.C.).

<sup>5</sup> Kerr, *Searches and Seizures in a Digital World*, *supra* at 569. See also Lesley Taylor, "The astonishing amount of personal data police can extract from your smartphone," (February 28, 2013), The Star.com online: <[www.thestar.com/news/world/2013/02/27/the\\_awesome\\_amount\\_of\\_personal\\_data\\_police\\_can\\_extract\\_from\\_your\\_smartphone.print.html](http://www.thestar.com/news/world/2013/02/27/the_awesome_amount_of_personal_data_police_can_extract_from_your_smartphone.print.html)> (where a police search of a smart phone revealed 104 call logs, eight passwords, 422 text messages, six wireless networks, and 10,149 files of audio, pictures, text and videos — 378 of which were deleted).

<sup>6</sup> See Edward T.M. Garland & Donald F. Samuel, "The Fourth Amendment and Computers: Is a Computer Just Another Container or Are New Rules Required to Reflect New Technologies?" (2009) 14 Georgia Bar Journal 15 at 16; see also *R. v. Little*, [2009] O.J. No. 3278 at para. 96 (S.C.J.).

<sup>7</sup> *R. v. Cole*, *supra* at para. 48 (S.C.C.).

“intermingling” of those documents alongside intensely personal information that the government has no reasonable grounds to search or seize.<sup>8</sup> The problem is even more acute when we consider not just the single personal computer but a computer network. In larger companies and institutions, thousands of computers are connected to each other across cities, countries and continents via company network servers. These computer users share disk drives. In that context, if a warrant to search a computer is not limited by protocols, it can potentially permit the police to comb through the information of thousands of innocent people. (The decision of the U.S. Court of Appeals for the Ninth Circuit in *United States v. Comprehensive Drug Testing Inc.* (“CDT”) illustrates this danger and the importance of search protocols in mitigating these risks.<sup>9</sup>)

9. ***The Inversion of the Search and Seizure Process.*** 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; if the police are looking for an elephant, they cannot reasonably search a matchbox.<sup>10</sup> 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.<sup>11</sup> Police then often take a mirror image of the entire hard drive so that they can search through its contents.<sup>12</sup> As a result, overseizure is a particularly acute problem in this context.<sup>13</sup> Computer searches involve “seiz[ing] the haystack to look for the needle.”<sup>14</sup> The physical world has built-in search protocols; the virtual world requires us to impose protocols in order to prevent the breadth of the computer search from being limitless.

## **B. Types of Search Protocols**

10. Search protocols can involve myriad possibilities. They can define, and thereby constrain, the search for specified keywords, file types, and date ranges; they can limit the search to text files or graphics files; and they can focus on certain software programs.<sup>15</sup> They can also prescribe the use of more sophisticated search tools based on constantly evolving forensic technologies that allow law

---

<sup>8</sup> See, e.g., *R. v. Cole*, *supra* at para. 88 (S.C.C.) (illegal photographs intermingled with photographs of the accused’s wife); *In the Matter of the Search of 3817 W. West End*, 321 F. Supp. 2d 953 at 958 (N.D. Ill. 2004); *United States v. Otero*, 563 F.3d 1127 at 1132 (10th Cir. 2009).

<sup>9</sup> *Comprehensive Drug Testing Inc.*, *supra* at 1165-67 (9th Cir. 2010) (en banc).

<sup>10</sup> See Reasons of the B.C.C.A. at para. 47, Appellant’s Record (“AR”), Vol. I, p. 52.

<sup>11</sup> *In the Matter of the Search of 3817 W. West End*, *supra* at 958 (N.D. Ill. 2004).

<sup>12</sup> *R. v. Cole*, *supra* at para. 5 (S.C.C.); *R. v. Little*, *supra* at para. 137 (Ont. S.C.J.).

<sup>13</sup> See *R. v. Jones*, [2011] O.J. No. 4388 at para. 68 (C.A.).

<sup>14</sup> *United States v. Hill*, 459 F.3d 966 at 975 (9th Cir. 2006).

<sup>15</sup> *In the Matter of the Search of 3817 W. West End*, *supra* at 959 (N.D. Ill. 2004).

enforcement to conduct computer searches without opening files by searching based on “file headers”<sup>16</sup> or “hash values”.<sup>17</sup> Some of those programs, such as Guidance Software’s “EnCase Forensic Toolkit”, are already used by law enforcement throughout Canada and other jurisdictions.<sup>18</sup>

11. In certain cases, such as *CDT*<sup>19</sup> or this Court’s decision in *Lavallee, Rackel & Heintz v. Canada (Attorney General)*<sup>20</sup> (where privilege in addition to privacy was at issue), search protocols may require a bifurcated investigation. The United States Department of Justice Guidelines for computer searches acknowledge that, where the computers seized contain vast amounts of highly confidential or privileged information unrelated to the investigation — *e.g.*, where the target of the search is a law firm’s or medical office’s computers — officers unconnected with the investigation should conduct an initial review of materials to separate out the material specified in the warrant.<sup>21</sup> These officers, known as a “filter team” or “taint team”, set up an ethical wall between the fruits of the search and the case officers, permitting only unprivileged, relevant files to pass over the wall. In particularly sensitive cases, search protocols may require the appointment of a neutral party to review the files and segregate data before investigating officers gain access to the evidence.

12. While the specific protocols will differ on a case-by-case basis, the approval of some kind of protocol should be required in every case. If law enforcement believes that the facts of the particular case do not justify *any* search restrictions, then it should bear the onus of persuading the issuing justice of this. The police should bear this onus because they “have available to them the necessary software, technology and expertise to enable them to tailor their searches in a fashion that

---

<sup>16</sup> 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, the computer and forensic software will not be fooled because the file header will reveal the true nature of the file. 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 750.

<sup>17</sup> A “hash value” for a file is an identifier that characterizes a data set. The relationship between a hash value and its data set compares roughly the relationship between an organism and its DNA sequence or fingerprint. See *R. v. Braudy*, [2009] O.J. No. 347 at para. 21 per Stinson J. (S.C.J.) (explaining that the hash value “is a unique number [of a digital file] that could only be the product of applying the same formula to an identical file: it is a so-called ‘digital fingerprint’”); see also 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 326-27; Kerr, “Searches and Seizures in a Digital World,” *supra* at 544-46.

<sup>18</sup> See Palumbo, “How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment” *supra* at 1001; see also *R. v. Little*, *supra* at para. 27 per Fuerst J. (Ont. S.C.J.) (describing officer’s testimony regarding EnCase forensic software).

<sup>19</sup> *Comprehensive Drug Testing Inc.*, *supra* (9th Cir. 2010).

<sup>20</sup> *Lavallee, Rackel & Heintz v. Canada (Attorney General)*, [2002] 3 S.C.R. 209 at paras. 4-7, 38-49.

<sup>21</sup> See, *e.g.*, “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”, online: U.S. Department of Justice <[www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf](http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf)> at 110.



will generate the information they seek, if it exists, while at the same time minimizing the intrusion on the computer user's privacy rights in other information stored on the computer."<sup>22</sup>

### C. Authority for Search Protocols

13. The BCCLA's proposal for computer search protocols is not a novel proposition in Canadian law. In *R. v. Polius*,<sup>23</sup> Justice Trafford suggested guidelines for *ex ante* search protocols. He remarked that "[t]he issuing justice could, if necessary, place conditions on the warrant to ensure that the search was conducted by a named person who was technologically capable of conducting the search, in the presence of a named officer who was knowledgeable about the investigation of the alleged crime or, in some cases, the issuing judge for an *ex parte* determination of what information in the cell phone, or computer, may be seized." Such a procedure would ensure that the privacy interests of the accused "would be optimally cared for" and the principle of "minimization would be respected throughout this process."<sup>24</sup>

14. In *R. v. Cross*,<sup>25</sup> the issuing justice recognized that the police had reasonable grounds to search the suspect's laptop only with respect to an e-mail purportedly received by the accused on August 6, 2005. Accordingly, the warrant contained a protocol that the police shall "limit search to information concerning e-mail of August 6, 2005...."<sup>26</sup> Once in possession of the laptop, however, the police proceeded to conduct a comprehensive forensic sweep of the entire computer, and uncovered images and video that appeared to be child pornography. Justice Brennan held that failure to adhere to the warrant's protocol amounted to a s. 8 violation because "unlimited authorization to search a personal computer is an invasion of anyone's privacy."<sup>27</sup>

15. The reasoning of the Ontario Court of Appeal in *R. v. Jones* supports search protocols. In *Jones*, Justice Blair rejected the notion that a computer, once seized, was an indivisible object subject to whatever testing the police may determine necessary.<sup>28</sup> Instead, he held that "computers are different from other more traditional objects of search and seizure."<sup>29</sup> Therefore, a warrant authorizing the search for evidence of fraud in a computer did not authorize a further search for

---

<sup>22</sup> *R. v. Jones*, *supra* at para. 50 (Ont. C.A.).

<sup>23</sup> *R. v. Polius*, [2009] O.J. No. 3074 (S.C.J.).

<sup>24</sup> *R. v. Polius*, *supra* at para. 57 (Ont. S.C.J.).

<sup>25</sup> *R. v. Cross*, [2007] O.J. No. 5384 (S.C.J.).

<sup>26</sup> *Ibid.* at para. 21.

<sup>27</sup> *Ibid.* at para. 27.

<sup>28</sup> *R. v. Jones*, *supra* at paras. 45, 52 (Ont. C.A.).

<sup>29</sup> *Ibid.* at para. 51.

evidence of child pornography.<sup>30</sup> Rather, a “computer search pursuant to a warrant must be related to the legitimate targets respecting which the police have established reasonable and probable grounds, as articulated in the warrant.”<sup>31</sup> Search protocols assist in achieving this objective. (Justice Blair did, however, also suggest that the police should not be constrained in the types of files they are permitted to search because the true file types may be disguised.<sup>32</sup> For the reasons set out in para. 19, *infra*, the BCCLA submits that this part of the opinion (which was *obiter dicta*) was wrong.)

16. In addition, search protocols are supported by established principles of search and seizure in Canadian law, including the *particularity* and *minimization* requirements. Even in the pre-*Charter* era, this Court held that justices have the power to limit and place conditions on the time, place and manner of execution of warrants.<sup>33</sup> In the *Charter* era, courts have required that warrants describe the item(s) to be seized with sufficient particularity.<sup>34</sup> Particularity is intimately connected to minimization, which requires that the search “should be conducted in a sensitive manner and be minimally intrusive.”<sup>35</sup> As noted above (see *supra* at para. 9), in the physical world, the particularized description of the object to be searched limits where law enforcement can look for it and can help minimize the invasiveness of the search. In the virtual world, however, the mere description of the particular items to be seized does not impose inherent restrictions. Search protocols do for computer searches what the particularity requirement does for the physical world: They help ensure that computer searches do not become unchecked fishing expeditions.

17. The U.S. case law is instructive. Certain U.S. jurisdictions have required approval of a search protocol as a prerequisite to the issuance of a warrant to search a computer.<sup>36</sup> Those decisions are grounded in the Fourth Amendment’s particularity requirement and the need to prevent warrant searches from becoming general exploratory searches.<sup>37</sup> Other courts have authorized

---

<sup>30</sup> *Ibid.* at para. 52.

<sup>31</sup> *Ibid.* at para. 42.

<sup>32</sup> *Ibid.* at para. 43.

<sup>33</sup> *Descôteaux et al. v. Mierzwinski*, [1982] 1 S.C.R. 860 at 889 (“The justice of the peace, in my view, has the authority, where circumstances warrant, to set out execution procedures in the search warrant.”).

<sup>34</sup> *Re Church of Scientology and the Queen (No. 6)* (1987), 31 C.C.C. (3d) 449 at 509-516 (Ont. C.A.) (cited with approval in Reasons of the B.C.C.A. at paras. 49-50, Appellant’s Record (“AR”), Vol. I, pp. 53-54).

<sup>35</sup> *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393 at para. 54; *R. v. Garofoli*, [1990] 2 S.C.R. 1421 at 1468-69.

<sup>36</sup> *In the Matter of the Search of 3817 W. West End*, *supra* at 954-957 (N.D. Ill. 2004).

<sup>37</sup> *Ibid.* at 957-959.

search protocols but have stopped short of creating a bright line rule.<sup>38</sup> The BCCLA submits that the optimal approach is to require a search protocol unless law enforcement can discharge its onus of persuading the issuing justice that the specific circumstances of the case make a search protocol unreasonable.

#### **D. The Criticism of *Ex Ante* Search Protocols Is Unavailing**

18. The main arguments against protocols are: defendants may have taken steps to disguise incriminating evidence; forensic analysts rarely know ahead of time exactly how they will attack a hard drive; justices of the peace are ill-equipped to define search protocols; and *ex ante* regulation is more costly and time consuming.<sup>39</sup> These arguments, however, are not so much against search protocols as they are in favour of *properly tailored* search protocols.

19. First, while criminals will attempt to disguise their files, forensic technology (which is constantly evolving) already has the means to deal with this challenge. As noted above, forensic software currently available to police allows analysts to conduct searches based on “file headers” or “hash values”.<sup>40</sup> The police can then, for example, compare those hash values found in the computer files against databases of hash values known to be child pornography.<sup>41</sup> Changing the name of the file or file extension will not thwart this search method.

20. Second, the fact that issuing justices are not computer experts is immaterial. We frequently ask judges to make decisions based on complex or scientific evidence.<sup>42</sup> It is incumbent upon the officer seeking the warrant — who should have some expertise (or at least access to expertise) on computers — to educate the issuing justice on how computers work and why a given search strategy is necessary.

21. Third, while law enforcement may not always know *ex ante* precisely what search methods they will require to conduct the search, there is nothing to prevent an investigating officer from going back to the issuing justice and saying, “*We have done all we can do under these present*

---

<sup>38</sup> *Comprehensive Drug Testing Inc.*, *supra* at 1178-1180 per Kozinski C.J. (concurring) (9th Cir. 2010); *In Re Appeal of Application for Search Warrant*, 2012 VT 102 at 7, 26-32 (Sup. Crt VT); *United States v. Carey*, 172 F.3d 1268 at 1274-76 (10th Cir. 1999); *United States v. Turner*, 169 F.3d 84 at 88 (1st Cir. 1999).

<sup>39</sup> Crown Factum at paras. 125-128; *R. v. Jones*, *supra* at paras. 39-43 (Ont. C.A.); Kerr, “Searches and Seizures in a Digital World,” *supra* at 544-45, 565-66, 576.

<sup>40</sup> See *supra* at para. 10.

<sup>41</sup> *R. v. Braudy*, *supra* at paras. 21-23 (S.C.J.).

<sup>42</sup> Daniel J. Solove, “Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference” (2005-2006) 74 *Fordham L. Rev.* 747 at 771-72.

*search protocols; here is what we have uncovered and here is why we need to resort to broader search techniques.”* The investigation will not be prejudiced by requiring this additional step because the data storage device will typically already be in the possession of law enforcement.<sup>43</sup> There is no danger of evidence being lost or destroyed.

22. In contrast, there is considerable advantage to requiring an *ex ante* protocol rather than simply relying on *ex post* review of police actions. *Ex ante* protocols will make it easier for the police to do their job because they will know the ground rules before they do it. *Ex ante* protocols will also avoid unnecessary litigation and save considerable time and resources. If law enforcement submits to reasonable search protocols before the search, then accused persons are less likely to find grounds for a *Charter* challenge after the search.

23. Finally, search protocols can also help law enforcement ensure the integrity of evidence by requiring computer searches to be done in controlled laboratory settings by technically trained officers. Computers are sophisticated devices. Improper handling — or even manual computer searches done outside of the laboratory setting — can damage or destroy evidence.<sup>44</sup> Simply opening a file or turning on a computer can overwrite deleted data, and may alter time stamps on the data which show when the suspect created or last accessed a file.<sup>45</sup>

24. In this case, for example, the officer performed a manual search on the Appellant’s computer.<sup>46</sup> This was unwise. If the time that the computer was accessed or the time when the accused last entered the dwelling were at issue, the officer could have compromised that evidence simply by accessing the computer. The manual search of a computer is the equivalent of walking into a murder scene with muddy boots and removing bare-handed a knife from the victim and dropping it in one’s coat pocket. Search protocols can help law enforcement address these risks.

## II. COMPUTER SEARCHES SHOULD REQUIRE “INVESTIGATIVE NECESSITY”

25. Due to the extreme invasiveness of computer searches (see *supra* at paras. 6-7), the Court should adopt a higher constitutional standard for a computer search warrant than the *reasonable and*

---

<sup>43</sup> See *R. v. Jones*, *supra* at para. 36 (Ont. C.A.) (“Searches of this nature are generally performed off-site and post seizure... Frequently, as here, there is no urgency. In such circumstances, nothing prevents the police from applying for another warrant.”).

<sup>44</sup> Schuck, “A Search for the Caselaw to Support the Computer Search Guidance in *United States v. Comprehensive Drug Testing*”, *supra* at 751.

<sup>45</sup> Robinton, “Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence” *supra* at 324-25.

<sup>46</sup> Reasons of the B.C.C.A. at para. 18, AR, Vol. I, p. 44.

*probable grounds* threshold ordinarily required for obtaining a search warrant.<sup>47</sup> The Court should require that law enforcement demonstrate *investigative necessity*.

26. The investigative-necessity standard is constitutionally required for what was traditionally viewed as being the most invasive search: wiretapping. As this Court stated in *Araujo* in the wiretapping context, “the investigative necessity requirement embodied in s. 186(1) is one of the safeguards that made it possible for this Court to uphold these parts of the *Criminal Code* on constitutional grounds.”<sup>48</sup> (The concept of necessity is also critical to the constitutionality of strip searches — another highly intrusive form of police search.<sup>49</sup>)

27. In light of this Court’s statement in *Morelli* that “it is difficult to imagine a more intrusive invasion of privacy than the search of one’s home and personal computer”,<sup>50</sup> investigative necessity should also now be required for computer searches. The wiretapping regime in Part VI of the *Criminal Code* reflects an understanding that there is no way to intercept incriminating communications without listening to private, intimate, and personal communications. Equally, with computer searches, it is difficult to perform targeted or isolated searches.

28. In addition, much of the information that wiretapping could uncover when it first emerged can now be discovered through computer searches. When wiretapping was first introduced as an investigative technique, people communicated largely by telephone. Today, people often communicate through email, instant messaging and social networking. All of these communications leave a digital trail in our computers.<sup>51</sup> (In this case, the Constable who conducted the search found that “MSN Messenger” and “Facebook” — two common modes of digital communication — were running on the Appellant’s computer.<sup>52</sup>) Thus, information that in the past was obtainable only through wiretapping is now easily available through a computer search. Indeed, a computer search is even more invasive because it can reach back and capture all of our electronic communications dating back to when we first started using the computer. A purposive approach to s. 8 should

---

<sup>47</sup> Under s. 487(1), a peace officer must only be satisfied that there are “reasonable grounds to believe” that there is a evidence of a crime or offence-related property in a “building, receptacle or place.”

<sup>48</sup> *R. v. Araujo*, [2000] 2 S.C.R. 992 at para. 26 per LeBel J. See also *R. v. S.A.B.*, [2003] 2 S.C.R. 678 at para. 53. See *contra*, *R. v. Lergie*, [2010] O.J. No. 3384 at para. 46 per Watt J.A. (C.A.).

<sup>49</sup> *R. v. Golden*, [2001] 3 S.C.R. 679 at para. 98.

<sup>50</sup> *R. v. Morelli*, *supra* at paras. 2, 105 (S.C.C.).

<sup>51</sup> See *supra* at para. 6.

<sup>52</sup> Ruling of the B.C.S.C. at para. 19, AR Vol. I, p. 148.

therefore require at least the same constitutional standard for computer searches as that which is required for wiretapping.

29. We acknowledge that this Court rejected investigative necessity as a constitutional requirement for the use of DNA warrants under ss. 487.04 to 487.09 of the *Criminal Code*. But the Court did so on the basis that DNA searches, unlike wiretaps, are target-specific whereas wiretaps are “sweeping in their reach” and “invariably intrude into the privacy interests of third parties who are not targeted by the criminal investigation.”<sup>53</sup> Computer searches are similarly sweeping and similarly intrusive of third party privacy interests.

30. The imposition of an investigative necessity requirement will not create an undue burden on the police. As this Court clarified in *Araujo*, investigative necessity does not mean that the tool in question can only be used as a “last resort”.<sup>54</sup> It simply means that there must be “practically speaking, no other reasonable alternative method of investigation in the circumstances of the particular criminal inquiry”.<sup>55</sup> In addition, the investigation of some offences will inevitably culminate in a computer search (*e.g.*, accessing child pornography). The investigative necessity requirement will not, therefore, be unduly onerous on the state.

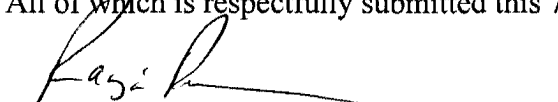
#### **PART IV: SUBMISSIONS ON COSTS**

31. The BCCLA does not seek costs and asks that none be awarded against it.

#### **PART V: NATURE OF THE ORDER REQUESTED**

32. The BCCLA respectfully requests leave to present oral argument for no more than 10 minutes at the hearing of this appeal.

All of which is respectfully submitted this 7<sup>th</sup> day of March, 2013.

  
 for: **NADER R. HASAN / GERALD CHAN**  
**Ruby Shiller Chan Hasan, Barristers**

*Counsel for the BCCLA*

<sup>53</sup> *R. v. S.A.B.*, *supra* at para. 54 (S.C.C.).

<sup>54</sup> *R. v. Araujo*, *supra* at paras. 34-35 (S.C.C.).

<sup>55</sup> *Ibid.*, at para. 29.

## PART VI: TABLE OF AUTHORITIES

<b>Case Law</b>	<b>Paras.</b>
<i>R. v. Morelli</i> , [2010] 1 S.C.R. 253	3, 7, 27, 28
<i>United States v. Comprehensive Drug Testing Inc.</i> , 621 F.3d 1162 (9th Cir. 2010) (en banc)	6, 8, 11, 17
<i>R. v. Cole</i> , [2012] S.C.J. No. 53 (S.C.C.)	7, 8, 9
<i>R. v. Little</i> , [2009] O.J. No. 3278 (S.C.J.)	7, 9, 10
<i>Lavallee, Rackel &amp; Heintz v. Canada (Attorney General)</i> , [2002] 3 S.C.R. 209	11
<i>In the matter of the Search of 3817 W. West End</i> , 321 F. Supp. 2d 953 (N.D. Ill. 2004)	8, 9, 10, 17
<i>United States v. Otero</i> , 563 F. 3d 1127 (10th Cir. 2009)	8
<i>R. v. Jones</i> , [2011] O.J. No. 4388 (C.A.)	9, 12, 15, 18, 21
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)	9
<i>R. v. Braudy</i> , [2009] O.J. No. 347 (S.C.J.)	10, 19
<i>R. v. Polius</i> , [2009] O.J. No. 3074 (S.C.J.)	13
<i>R. v. Cross</i> , [2007] O.J. No. 5384 (S.C.J.)	14
<i>Descôteaux et al. v. Meirzwinski</i> , [1982] 1 S.C.R. 860	16
<i>Re Church of Scientology and the Queen (No. 6)</i> (1987), 31 C.C.C. (3d) 449 (Ont. C.A.)	16
<i>R. v. M. (M.R.)</i> , [1998] 3 S.C.R. 393	16
<i>R. v. Garofoli</i> , [1990] 2 S.C.R. 1421	16
<i>In Re Appeal of Application for Search Warrant</i> , 2012 VT 102 (Sup. Crt VT)	17
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999)	17
<i>United States v. Turner</i> , 169 F.3d 84 (1st Cir. 1999)	17
<i>R. v. Araujo</i> , [2000] 2 S.C.R. 992	26, 30
<i>R. v. S.A.B.</i> , [2003] 2 S.C.R. 678	26, 29
<i>R. v. Lergie</i> , [2010] O.J. No. 3384 (C.A.)	26
<i>R. v. Golden</i> , [2001] 3 S.C.R. 679	26

**Commentary**

- “Hard Drives”, online: PC Mag.com 6
- Orin S. Kerr, “Searches and Seizures in a Digital World” (2005) 119 Harv. L. Rev. 531 6, 7, 10, 18, 19
- Marc Palumbo, “How Safe is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment”, (2009) 36 Fordham Urb. L.J. 977 10
- Lesley Taylor, “The astonishing amount of personal data police can extract from your smartphone” online: The Star.com 7
- Edward T.M. Garland & Donald F. Samuel, “The Fourth Amendment and Computers: Is a Computer Just Another Container or Are New Rules Required to Reflect New Technologies?” (2009) 14 Georgia Bar Journal 15 7
- 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 10, 23
- 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 10, 23
- “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”, online: U.S. Department of Justice 11
- Daniel J. Solove, “Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference”, (2005-2006) 74 Fordham L. Rev. 747 20