Comment

A DATABASE TOO FAR? INTERPRETING THE COMPETITION BUREAU'S COMPUTER SEARCH POWERS

Casey W. Halladay & Joshua Chad[1]

The Competition Bureau possesses a formidable arsenal of investigative powers. One of those tools is an extremely broad—in the authors' view, overbroad—power when executing a search warrant to access and seize records or data stored outside of Canada that are available to computer systems located at the Canadian search site. This article reviews the origin and nature of the "long-arm" computer search powers available to the Bureau, key Canadian jurisprudence in this area, and argues that a restricted interpretation of these powers better reflects both the relevant jurisprudence and Parliamentary intent.

Le Bureau de la concurrence possède un formidable arsenal de pouvoirs d'enquête. L'un de ces outils est un pouvoir extrêmement large, beaucoup trop large aux yeux des auteurs, de perquisitionner en vue d'accéder à des dossiers ou données conservés à l'étranger, et de les saisir, lorsqu'ils sont disponibles dans un système informatique situé sur le lieu de la perquisition au Canada. Cet article passe en revue les origines et la nature des pouvoirs de perquisition informatique « longue distance » à la disposition du Bureau et la jurisprudence canadienne de principe en la matière. Les auteurs soutiennent qu'une interprétation restrictive de ces pouvoirs reflète mieux la jurisprudence pertinente et l'intention du législateur.

I. Introduction

It is well-known that Canadian Competition Bureau ("Bureau") officials, like their peers in other antitrust agencies, have a broad arsenal of powers under the *Competition Act*[2] for investigating anti-competitive conduct within Canada. What is generally less well-known is the range of tools available to the Bureau that purport to

allow it to obtain information located abroad.[3] One of those tools is an extremely broad—in our view, overbroad—power when executing a search warrant to access and seize records or data stored outside of Canada that are available to computer systems located at the Canadian search site. This article reviews the origin and nature of the "long-arm" computer search powers available to the Bureau, key Canadian jurisprudence in this area, and advocates that a restricted interpretation of these powers would better reflect both the relevant caselaw and Parliamentary intent.

II. The Legislative Framework For Bureau Computer Searches

Two search warrant regimes are available to the Bureau, under the *Competition Act* and the *Criminal Code*.[4] The relevant provisions of each regime provide as follows:

Competition Act

> 16. (1) A person who is authorized pursuant to subsection 15(1) to search premises for a record may use or cause to be used any computer system on the premises to **search any data** contained in or **available to the computer system**, may reproduce the record or cause it to be reproduced from the data in the form of a printout or other intelligible output and may seize the printout or other output for examination or copying.
>
> (2) Every person who is in possession or control of any premises in respect of which a warrant is issued under subsection 15(1) shall, on presentation of the warrant, permit any person named in the warrant to use or cause to be used any computer system or part thereof on the premises to **search any data** contained in or **available to the computer system** for data from which a record that that person is authorized to search for may be produced, to obtain a physical copy thereof and to seize it.[5]

Criminal Code

> 487(2.1) A person authorized under this section to search a computer system in a building or place for data may

(a) use or cause to be used any computer system at the building or place to **search any data** contained in or **available to the computer system**;

(b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;

(c) seize the print-out or other output for examination or copying; and

(d) use or cause to be used any copying equipment at the place to make copies of the data.

(2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search

(a) to use or cause to be used any computer system at the building or place in order to **search any data** contained in or **available to the computer system** for data that the person is authorized by this section to search for;

(b) to obtain a hard copy of the data and to seize it; and

(c) to use or cause to be used any copying equipment at the place to make copies of the data.[6]

Notably, both regimes authorize investigators to search for and seize "*any data contained in or available to the computer system*." On the plain language of the legislation, this would appear to include searches for and seizure of data or records saved on a server located outside of Canada, so long as such data or records were accessible from (i.e., "*available to*") the computer system located at the search premises in Canada. Both regimes also explicitly compel any person who is "*in possession or control*" of the premises under search to permit such a search or seizure.

The *Competition Act* computer search provisions date to 1986 when, following the "Stage II" reforms,[7] the federal government transformed

the predecessor *Combines Investigation Act* into the *Competition Act* with the passage of then-Bill C-91.[8] There is little evidence in *Hansard*, or the minutes of the Legislative Committee that assisted in drafting the Bill, to suggest that legislators considered the broad implications of the language "*available to the computer system*" at the time.[9] Indeed, the minutes reflect only a brief and general discussion of the scope of these powers. Mr. Mel Cappe, of the Department of Consumer and Corporate Affairs, noted that the Commissioner's (then the Director of Investigation and Research) computer search powers could be restricted at the issuing judge's discretion, and the target of the search could subsequently apply to a judge to have the scope of a warrant narrowed.[10]

Commentary from the Bureau on the scope of these powers has been sparing since their inception in 1986. In a 2004 conference paper, two Bureau employees asserted that section 16 of the *Competition Act* permits the search of computer systems in Canada for "*records in foreign data bases.*"[11] Additionally, in a 2008 Information Bulletin discussing the search warrant provisions of the *Competition Act*, the Bureau more generally stated that "*data that are accessible via [a] computer system can be searched even if the data are not located on the premises.*"[12] We are not aware of any other public record commentary from the Bureau on the geographic scope of its computer search powers.[13]

III. Jurisprudence On The Scope Of Computer Search Powers

In recent years, Canadian courts have issued decisions supporting a relatively broad interpretation of the power to search and seize records and data stored outside of Canada. In a tax case involving the online retailer, eBay, the Federal Court of Appeal accepted the premise that information stored electronically outside Canada "*cannot truly be said to 'reside' only in one place.*"[14] In that case, the Canada Revenue Agency sought to obtain certain electronic records relating to Canadian customers of eBay, with eBay Canada Ltd. resisting on the grounds that the records did not exist in Canada and were thus unavailable to the Minister of National Revenue. The trial judge, whose reasons were upheld by the Federal Court of Appeal, analyzed the situation as follows:

> when information, though stored electronically outside Canada, is **available to and used by those in Canada**, [the law] must be approached from the point of view of the realities of today's

> world [...] The reality is that **the information is readily and instantaneously available** to those within the group of eBay entities in a variety of places. It is **irrelevant where the electronically-stored information is located** or who as among those entities, if any, by agreement or otherwise asserts "ownership" of the information.[15]

Notably, on appeal the Federal Court of Appeal explicitly rejected eBay's suggestion that only data or records accessed from Canada and physically saved to computers at the Canadian search site are "*located in Canada*." Taking a practical approach, Justice Evans, speaking for the court, countered that:

> [c]ounsel concedes that the information [...] would be located in Canada if the appellants had downloaded it to their computers. In my view, it is formalistic in the extreme for the appellants to say that, until this simple operation is performed, the information which they lawfully retrieve in Canada from the servers, and read on their computer screens in Canada, is not located in Canada.[16]

A detailed analysis of the trial and appellate decisions reveals that both Justice Hughes and Justice Evans focused on the actual use of offshore data by Canadian-based employees in their respective decisions justifying an investigator's ability to search and seize materials located outside Canada. For example, in the Federal Court trial decision, Justice Hughes stated that:

> [t]he more important issue in the circumstances of this case is **the ability, particularly of eBay Canada, to access and use the information** [...] eBay Canada **in fact does access that information and use it** in the course of its business operations in Canada.[17]

> [...] Here **eBay Canada has access to and uses information stored in a computer** for the very purpose of dealing with Canadian Power Sellers. For perhaps corporate efficiency the information is stored elsewhere, **but its purpose is in respect of Canadian business.**[18]

Similarly, in the Federal Court of Appeal decision, Justice Evans noted that:

> with the click of a mouse, **the appellants make the information appear on the screens on their desks in Toronto and Vancouver, or anywhere else in Canada.** It is **as easily accessible as documents in their filing cabinets in their Canadian offices.** Hence, it makes no sense in my view to insist that information stored on servers outside Canada is as a matter of law located outside Canada.[19]

A similar line of reasoning was adopted by the Ontario courts in *R v Edwards*,[20] where Justice LaForme held that a search is not unreasonable when data is remotely seized from computer storage units that are not at the location specified in the warrant. In reaching this conclusion, Justice LaForme held that:

> [i]n my view, in this day and age, with the development of computer technology and the so called "information highway," information exists where it is capable of being **accessed, translated and recorded.**[21]

Justice LaForme supported his view by referencing the language of section 487(2.2) of the *Code* (excerpted at Part II above) and, in particular, the "available to" language that also appears in the search warrant regime under the *Competition Act*.[22]

In our view, this aspect of the courts' analysis should limit the breadth of Bureau computer searches. In particular, offshore data and records that are not regularly accessed and used by Canadian employees in carrying out their duties should fall outside the scope of the eBay decisions. The *eBay* excerpts provided above support our interpretation as they refer to "*information, though stored electronically outside Canada, [that] is* ***available to and used by those in Canada***" and expressly state that "*[t]he* ***more important issue*** *in the circumstances of this case* ***is the ability****, particularly of eBay Canada,* ***to access and use the information.***" In effect, the court appears to have granted the Minister of Revenue access to the "*foreign*" data as it was, practically speaking, part of the Canadian business. From the facts set out in the decision, eBay Canada Ltd. employees apparently accessed the relevant data

on a regular basis and used it in the daily operation of the Canadian business.

Conversely, where a Canadian company may have access to data or records held by a foreign affiliate offshore, but does not regularly access such materials or the materials play no role in the daily operations of the Canadian business, we believe that the jurisprudence supports our view that such data or records should not be accessible to a Bureau computer search. Our interpretation is more consistent with the principles underpinning the *eBay* decisions, and provides a more nuanced response to the dynamics of the present-day computer search environment. For example, the Bureau employs forensic search experts with specialized experience and technical skills that allow them to locate and access information that an average employee may not. Indeed, such persons are often included among a search team's personnel for precisely this purpose. Moreover, courts have expressly permitted Bureau officials to utilize specialized computer search software to allow them to access data that might otherwise be inaccessible.[23]

In our view, the Bureau's computer search powers should be interpreted as applying only to those offshore data and records that are actually accessed or used by employees of the Canadian business in their daily functions, rather than all information that can conceivably be located by forensic search experts from a computer at the search site. As described more fully at Part IV below, such an interpretation is more consistent with recent jurisprudence from the Supreme Court of Canada on the law of computer searches generally.

IV. Closing The Gap Between Technology And The Law

In recent years, Canadian courts have debated whether computers are like any other receptacle within business premises, and can therefore be searched and data seized under the general warrant powers to search a given location. Some courts have held that computers should be treated as premises unto themselves requiring specific prior authorization within a warrant in order to be searched; others have effectively treated computers as equivalent to desks, filing cabinets, or other storage locations commonly found in an office environment.

Last year, the Supreme Court of Canada resolved this debate by

ruling, in the case of *R v Vu*, that computer (and cellular phone) searches require explicit prior authorization in a search warrant.[24] Justice Cromwell, writing for a unanimous court, concluded that the usual underlying policy assumptions that justify searches of all physical locations within a business premises do not apply to computers, as:

> computers are not like other receptacles that may be found in a place of search. The particular nature of computers calls for a specific assessment of whether the intrusion of a computer search is justified, which in turn requires prior authorization.[25]

The Court relied on privacy considerations as a key basis for requiring a separate, higher standard for computer searches, with Justice Cromwell remarking that:

> [t]he privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets. Computers **potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search**. These factors [...] call for specific pre-authorization in my view.[26]

As a result, specific and targeted pre-authorization allowing the search of computers and personal electronic devices[27] within the search warrant is required in order to ensure that the authorizing judge has expressly turned his or her mind to the unique privacy concerns that these searches raise.[28]

Justice Cromwell also expressed concern with the extremely broad range of information potentially available to computer searches that has been made available by the Internet:

> [w]hile documents accessible in a filing cabinet are always at the same location as the filing cabinet, the same is not true of information that can be accessed through a computer. The intervener the Canadian Civil Liberties Association notes that, when connected to the **Internet, computers serve as portals to an almost infinite amount of information that is shared**

> **between different users and is stored almost anywhere in the world. Similarly, a computer that is connected to a network will allow police to access information on other devices.** Thus, a search of a computer connected to the Internet or a network **gives access to information and documents that are not in any meaningful sense at the location for which the search is authorized.**[29]

In our view, the language highlighted above supports our argument that, consistent with the *eBay* principles, Bureau computer searches should be limited to only those offshore data and records that are actually accessed and used by Canadian-based employees, rather than all offshore information that can be located by the Bureau's forensic search experts. The *Vu* decision clearly articulates a concern that investigators may access "*vast amounts of information*" that: (1) employees "*cannot control*"; or (2) "*may not even be aware of*"; or (3) is not located "i*n any meaningful sense*" in the search location. Allowing Bureau officials to search and seize data or records located, for example, on the server of the Japanese parent company of a Canadian subsidiary would appear to violate each of these principles, unless the Bureau could demonstrate that the Canadian subsidiary was regularly accessing and using such data or records (as was the case in the *eBay* decisions). At a minimum, should Bureau officials wish to search and seize information stored offshore, we contend that they must seek specific pre-authorization to do so in the warrant from the issuing judge, in order to address the concerns identified by the Supreme Court of Canada in *Vu*.

While stipulating that computer searches require express pre-authorization, Justice Cromwell also provided a remedy for investigators executing warrants that do not explicitly authorize computer searches. In such a situation, investigators are permitted to seize any computers located on the search premises—provided they take the necessary measures to "*ensure the integrity of the data*" contained on the computers—pursuant to a basic search warrant.[30] The investigators may then apply to a court for specific authorization in order to search the computers.

The *Vu* decision also considered whether warrants to search computers and personal electronic devices require, *ex ante*, detailed "search protocols" setting out rules for searching the devices, with

the Supreme Court of Canada rejecting such a requirement on two grounds. First, it held that the manner in which a search is carried out is generally reviewed after the fact, with a complainant permitted to raise arguments as to whether the search was unreasonable. (This would ordinarily be the opportunity for a company whose offshore data or records were seized to raise the argument we have presented in this paper regarding a reasonable limit on the Bureau's computer search powers.) Second, requiring search protocols would add too much complexity to the search warrant process and create practical difficulties in effectively carrying out searches, as requiring a judge to, *ex ante*, predict which investigative techniques may be required and permitted to search the computers for the relevant information would be unduly burdensome.[31] However, the Court did note that, under certain circumstances and at the court's discretion, a protocol determined before the search may be justified. For example, the Court indicated that a protocol may be appropriate in the presence of "*confidential intellectual property or potentially privileged information.*"[32]

V. Conclusions

The law of computer (and personal electronic device) searches is clearly a continuously-evolving subject, with the jurisprudence struggling to match the pace of technological progress. In our view, the notion that Bureau investigators, including forensic search experts, can search and seize data and records located in offshore jurisdictions while executing a search warrant on Canadian premises is vulnerable to challenge. It is inconsistent with the position taken in the *eBay* decisions that offshore materials should be regularly used by Canadian employees in order to be considered to be "*located in Canada.*" More importantly, it directly engages the policy concerns raised by the Supreme Court of Canada in the *Vu* decision, *i.e.*, that investigators may be able to access "*vast amounts of information*" that employees "*cannot control*" or "*may not even be aware of*" and that is not located "*in any meaningful sense*" in Canada.

Interpreting section 16 of the *Competition Act* to permit such long-arm searches would also be anachronistic. The key computer search provisions date to 1985, an era of far less sophisticated technology than today, and have never been updated. Commercial Internet access was not yet available. Large-scale data storage, offshore servers, technology

outsourcing, and cloud computing did not exist. The ubiquity of the personal (or office) computer was still years away. As noted at Part II above, there is nothing in the *Hansard* debates or the preparatory materials for Bill C-91 to suggest that Parliament intended to create powers, arguably *ultra vires* its (and the Bureau's) own authority, to search and seize data and records located in another country. In a relatively contemporaneous article of September 1986, then-Director of Investigation and Research Cal Goldman wrote that section 16:

> also states that "any data contained in or available to the [computer] system" may be searched for. This permits the Director's representative to **gain access to company data stored at a location off the search premises, such as a service bureau or the head office of a corporation.** [33]

These comments must be understood in their proper context: as head of the Bureau, Mr. Goldman can be presumed to have adopted an expansive—rather than restrictive—view of his agency's search powers. More tellingly, he made these assertions years before the existence of commercial Internet access, and thus the comments can only be interpreted as applying to a "*service bureau*" or "*head office*" that was part of a network of linked domestic computers, rather than to data servers located overseas (which were not physically accessible at the time his article was written).

In summary, we contend that an expansive interpretation of the Bureau's computer search powers is inconsistent with both the guiding principles of the relevant jurisprudence, and Parliament's intent when creating these powers. Instead, the Bureau's computer search powers should be limited to seizing only those offshore data and records that are actually accessed or used by a Canadian business. Furthermore, at a minimum, any search and seizure of data or records stored on offshore servers should be expressly authorized by the terms of a search warrant prior to the search taking place.

Endnotes

[1] Casey W. Halladay, BA (Hons), MA, LLB, LLM, of the Bars of Ontario, New York, England & Wales, is a Partner at McMillan LLP, Toronto. Joshua Chad, HBA, JD, of the Ontario Bar, is an associate at McMillan LLP, Toronto.

[2] RSC 1985, c C-34 [*Competition Act*].

[3] On the Bureau's long-arm subpoena powers to compel the production of

overseas documents under section 11(2) of the *Competition Act*, see D Martin Low & Casey W Halladay, "Key Issues for Canadian Cartel Enforcement in 2012" (Paper delivered at the American Bar Association / International Bar Association International Cartel Workshop, 1-3 February 2012).

[4] RSC 1985, c C-46 [*Criminal Code*].

[5] *Supra* note 2, s 16 [emphasis added].

[6] *Supra* note 4, s 487(2.1)ff [emphasis added].

[7] See e.g. LW Hunter, "The *Competition Act* of 1986: A Land of Hope and Promise" (2012) 25:2 Can Comp L Rev 203.

[8] Bill C-91, *An Act to establish the Competition Tribunal and to amend the Combines Investigation Act and the Bank Act and other Acts in consequences thereof*, 1st Sess., 33rd Parl, 1986, (assented to 17 June 1986).

[9] House of Commons, *Minutes of Proceedings and Evidence of the Legislative Committee on Bill C-91*, No 9 (15 May 1986) at 9:34 and 10:72-73. These are the only two instances in which the computer search powers were discussed.

[10] *Ibid* at 10:72.

[11] See Mike Sullivan & Josée Filion, "The Basics of International Cartel Enforcement in Canada" (Paper prepared for the Osgoode Hall Continuing Legal Education Program, *Canada's Competition Regime: Thinking Strategically*, York University, 14 January 2004), at 6.

[12] Competition Bureau of Canada, *Information Bulletin on Sections 15 & 16 of the Competition Act* (25 April 2008), online: <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/02660.html>.

[13] See also *infra* note 33.

[14] *eBay Canada Ltd. v M.N.R.*, 2008 FCA 348 at para 51.

[15] *eBay Canada Limited v Canada (National Revenue)*, 2007 FC 930 at para 23 [emphasis added].

[16] *Supra* note 14 at para 50.

[17] *Supra* note 15 at para 12 [emphasis added].

[18] *Ibid* at para 25 [emphasis added].

[19] *Supra* note 14 at para 48.

[20] [1999] OJ No 3819 (SCJ).

[21] *Ibid* at paras 89-90 [emphasis added].

[22] *Ibid.*

[23] See e.g. *United States Pipe & Founding Co. (Re)* (1994), 58 CPR (3d) 463 at paras 11-13 (Ont Gen Div).

[24] 2013 SCC 60 [*Vu*].

[25] *Ibid* at para 39.

[26] *Ibid* at para 24 [emphasis added].

[27] Justice Cromwell explicitly included cellular telephones and other personal electronic devices within the scope of his computer search analysis, noting that "I do not distinguish, for the purposes of prior authorization, the computers from the cellular telephone in issue here. Although historically cellular phones were far more restricted than computers in terms of the amount and kind of information that they could store, present day phones

have capacities that are, for our purposes, equivalent to those of computers": See *ibid* at para 38.

[28] *Ibid* at para 47.

[29] *Ibid* at para 44 [emphasis added].

[30] *Ibid* at para 49.

[31] *Ibid* at paras 57-58.

[32] *Ibid* at para 62.

[33] Calvin S Goldman, "New Developments in the Enforcement of Canadian Competition Law" (Paper delivered at the Canadian Bar Association-Ontario and the Law Society of Upper Canada Continuing Legal Education Joint Programme: The *New Competition Act*, 26 September 1986), [*unpublished*] [emphasis added].