**The Compliance Conundrum in the Electronic Age: A Canadian Perspective**

By Melanie L. Aitken and Emrys Davis[[1]](#footnote-1)

Bennett Jones LLP

# Introduction

Twenty years ago, participants in the lysine cartel met in hotel rooms. Detecting and prosecuting that cartel took a whistleblower surreptitiously recording the meetings over a period of several months. Demonstrating just how far technology has come since then, the grainy, black and white videos are now available on YouTube.[[2]](#footnote-2)

The same information technology revolution which put the lysine videos on the Internet has had consequences for cartel detection. As business communication has migrated from in-person meetings or telephone calls to emails and Internet chat rooms, agreements between competitors are just as likely to be formed through electronic communication as in person.

That communication shift has important consequences for businesses as they fashion compliance programs to suit the information technology world. On the one hand, the prevalence of electronic communications may make detecting employees' anticompetitive activity easier. After all, many types of electronic communications can be monitored and permanently saved even if the employee has, for example, deleted the email. In contrast, identifying at large where one should monitor or seek to record communication is next to impossible unless, as in lysine, someone on the inside offers to assist.

On the other hand, if monitoring employees' activity via information technology is easier, the associated compliance burden is far greater. Before the growth of information technology, compliance programs could target and regulate employees in "high risk" situations. For example, events at which competitors would interact and thus create a potential of cartel activity could be vetted by the legal department or avoided all together. Thus, businesses could create employee conduct policies around trade shows or industry organization meetings, or perhaps even withdraw from industry organizations. Training could target employees who had pricing authority or potentially interacted with competitors.

In an information technology age, the potential venues for competitor interaction are legion. Bloomberg chat rooms, Facebook groups, and non-business email accounts all present opportunities for ongoing communication between competitors that may require more effort to detect and monitor (if the tools are even available).

In this context, businesses must weigh the burden associated with compliance in the information technology age against the risks of maintaining a potentially ineffective compliance program.

This paper focuses on Canada. It outlines the risks facing businesses whose compliance programs may not measure up against the tools available to the Competition Bureau (the "Bureau") to uncover electronic evidence of cartel activity. It also discusses the potential benefits for Canadian businesses of robust compliance programs.

# Risks to Businesses with potentially ineffective Compliance Programs

While information technology has increased the compliance burden, it has likewise increased the enforcement burden. While the government has not enjoyed a corresponding increase in resources, the Bureau still has powerful legal tools to discover electronic records of cartel activity, including records stored on servers outside Canada. Multinational businesses cannot rely on foreign-based servers to shelter their records from search by Canadian authorities. And once the information is in the Bureau's hands, the law in Canada provides several avenues for civil plaintiffs to access that information, typically to the detriment of defendants in civil proceedings. With settlements of Canadian class actions now growing into the tens of millions of dollars and a lower standard for class certification than in the United States (the "US"), civil antitrust actions present a growing area of risk for businesses operating in Canada.

## The Bureau's Powers to Search Electronic Evidence

The Bureau has the power to search computers under sections 15 and 16 of the *Competition Act[[3]](#footnote-3) (the "Act").* The *Act* permits a person authorized to conduct a search to "use or cause to be used any computer system on the premises to search any data contained in or available to the computer system…"[[4]](#footnote-4) This power is substantial. In a cloud computing age, computers often act as portals, allowing the person conducting the search to retrieve information available to the computer but not necessarily located on the computer.

While the breadth of the Bureau's search power has not been litigated as it relates to computer searches, case law in related areas suggests that the Bureau will not be limited to searching documents stored on the computer's hard drive, or even documents located in Canada. Rather, it is likely that the Bureau can search for and seize documents located on servers outside of Canada.

For example, the Federal Court of Appeal upheld an order requiring eBay to produce documents to the Canadian Revenue Agency, even though the documents were stored on eBay's servers in the US. The Court of Appeal noted that, while performing daily tasks at offices in Canada, employees of eBay accessed and used information located on severs in the US: "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."[[5]](#footnote-5) To employees, this information was "as easily accessible as documents in their filing cabinets in their Canadian offices"[[6]](#footnote-6). Thus, the Federal Court of Appeal upheld the trial decision, confirming that information stored electronically outside Canada, "cannot truly be said to 'reside' only in one place"[[7]](#footnote-7). It ordered eBay to disclose the electronically-stored information, finding it was "located" both on the server in the US as well as at the point of access in Canada.

Similarly, the Ontario Superior Court of Justice concluded that data contained, “in or available to the computer system”, included all relevant information that could be accessed by the computer. When it comes to computers, information “exists where it is capable of being accessed, translated and recorded”[[8]](#footnote-8). Thus, information located on a server in a foreign country that can be accessed, translated and recorded in Canada is deemed to be located in Canada as well.

In 2013, the Supreme Court of Canada entered the fray on whether authorities require specific judicial authorization to search computers, or whether a computer can be searched if it is found at the location to be searched. In *R v Vu*, the Supreme Court of Canada held that authorities can no longer automatically search a computer found at the location to be searched. Rather, they must obtain specific, prior authorization to search a computer. Computers had previously been searchable in the same way as all other receptacles at the site of the search. However, computers are not like all other receptacles. Justice Cromwell explained:

“Computers can 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.”[[9]](#footnote-9)

Requiring specific, prior authorization to search a computer ensures that judges authorizing warrants have considered the vast amount of information obtainable from a computer, and concluded that information should be searchable. This is an important protection for individuals against unreasonable search and seizure by the state.

However, *R v Vu* does not explicitly apply so as to restrict the scope of the Bureau's powers under section 15 and 16 of the *Act*. Should the Bureau obtain specific judicial authorization to search a computer, the broad scope of sections 15 and 16 make vulnerable foreign-located electronic documents if they can be accessed from a computer in Canada. Whether, as some authors have suggested, *R v Vu* will be interpreted so as to limit the scope of computer searches initiated under the *Act,* such that they do not become fishing expeditions, remains to be seen.[[10]](#footnote-10)

## Risk of Public Disclosure of Evidence Obtained by the Government

Criminal proceedings are the initial risk for businesses once the Bureau obtains potentially incriminating electronic records. While section 29 of the *Act* and the Bureau's practices and procedures ensure that information gathered in the context of a criminal investigation is confidential, the risk of such evidence getting into the hands of civil plaintiffs is real. Significantly, there are important exceptions to the general non-disclosure rule. These exceptions create risks for businesses who increasingly face follow on civil class actions, even if the criminal investigation never produces a conviction. In Canada, civil plaintiffs have at least three avenues through which to seek detailed information about criminal investigations for use in civil proceedings.

First, detailed information about the Bureau's investigation may be revealed when the Bureau seeks judicial authorization to obtain a search warrant or a civil production order. Such judicial authorization requires the Bureau to file an Information to Obtain ("ITO"), typically prepared by the investigating officer, which describes in detail the reasonable grounds to believe an offence has been committed and that there is evidence of the offence at the location sought to be searched. The ITO is filed publicly with the court, although the court file may be sealed until the warrant is executed so as not to prejudice the Bureau's investigation by tipping off the targets of the searches. The default rule, and where the risk arises, is that, after the search, the ITO will be available to the public. This presumption of open courts process applies generally to the contents of court files in Canada no less than in this context, and although the authorities can seek further sealing orders, they have enjoyed only mixed success in doing so thus far.

The availability of detailed information on alleged cartel activity through public ITOs has been used by civil plaintiffs in the past, most notably in the context of the Bureau's investigation into the chocolate industry. In that instance, US plaintiffs relied on the ITO to begin class proceedings in the US, only to have their action dismissed over six years later owing to a failure to present sufficient evidence of collusion.[[11]](#footnote-11) While ultimately a victory for the defendants, the disclosure of information in the ITO resulted in protracted and expensive civil litigation in the US, which might never have been initiated had the ITO been permanently sealed.

The Bureau has said that it will advocate for sealing orders that are as expansive as possible at the time it seeks the judicial authorization to search. More specifically and at a minimum, the Bureau will typically try to obtain sealing orders where the information could identify the immunity applicant. However, the prospect of expansive sealing orders, particularly ones going beyond the pure issue of the identity of an immunity applicant (and the question as to how much information reveals that identity is uneven) is not at all promising.

Second, unlike in the US where plea agreements typically describe the criminal conduct at a very high level, in Canada, the Crown and the party pleading guilty have traditionally filed detailed Statements of Admissions (the "Statement") to support a criminal conviction and joint sentencing submission. This Statement will often include detailed information about the conduct being pleaded to. For example, Statements filed to support conviction in several cases arising from the Bureau's sprawling auto parts investigation referred to the victims of the conduct, the specific vehicle models affected, time periods involved, detailed volume of commerce information, and even the other parties involved in the conduct. Not only can this information serve as a roadmap against the party pleading guilty, but by referring to others involved in the conduct, even a corporation that does not plead guilty might find itself named in a Statement as a co-conspirator or fellow bid-rigger.

Third, the Supreme Court of Canada recently held that wiretaps collected by the authorities in the context of criminal investigations can be accessed by civil plaintiffs through court-ordered disclosure.*[[12]](#footnote-12)* The Supreme Court determined that disclosure of the information in that case was consistent with the applicable principles: (1) the disclosure was limited in scope to protect the privacy of all those whose communications were intercepted; (2) disclosure of the information would not hinder the efficient conduct of the criminal proceedings or violate the right of the defendants still facing criminal charges to a fair trial; and (3) the order did not impose an undue financial and administrative burden on the third party in question.[[13]](#footnote-13)

Notably, the Supreme Court did not decide whether non-wiretap evidence collected by the Bureau in an investigation could also be subject to disclosure. Moreover, although Section 29 explicitly provides for confidentiality of the Bureau's record of investigation and prohibits disclosure of information obtained under a search warrant, it also contains a blanket exemption to that protection where disclosure is “for the purposes of the administration or enforcement of this Act,” meaning that, depending on the value ascribed to civil enforcement as promoting the *Act*, disclosure could be facilitated under this blanket authority, if, that is, the Bureau agreed.

Because the Supreme Court left this important question unanswered, it will fall to lower courts to determine the scope of the section 29 exemption. If the exemption is interpreted broadly, vast amounts of information obtained by the Bureau under the broad search and seizure powers could become accessible to civil plaintiffs. Information is also obtained by the Bureau from parties participating in the Bureau's Immunity and Leniency Programs. Before such information is disclosed to criminal accused in the context of the Crown's disclosure obligations, the Bureau will likely assert public interest or settlement privilege over that information. However, how the Bureau would treat information not obtained through these programs for the purposes of section 29 is less certain.

#  Benefits to Businesses with Robust Compliance Programs

The obvious benefit to businesses with robust compliance programs is avoiding violations of the *Act*. However, many businesses presume themselves to act within the law and do not have a history of violations. These businesses may question the value of a compliance program, particularly when the cost of such a program, as discussed above, may be growing significantly in the information technology age.

In Canada, beyond avoiding legal violations altogether, there are two important ways that robust compliance programs can benefit businesses and may tip the scales for some in deciding whether or not to invest in the process.

## Participation in the Immunity and Leniency Programs

The best result for any business is to never run afoul of the *Act*, and in particular, its criminal prohibitions on cartel activity such as price-fixing, market allocation, and bid-rigging. If avoiding violations is the best result, avoiding or significantly reducing liability is a close second. The Bureau's Immunity and Leniency Programs offer those benefits to corporations who come forward with information about a violation of the *Act's* criminal provisions and otherwise meet the requirements of the Programs. The first applicant to report the conduct is eligible to receive immunity from prosecution. Subsequent applicants may receive lenient treatment, typically a recommended percentage discount on the fine the Bureau would otherwise have recommended.

Compliance programs are important tools businesses can use to discover potential anticompetitive conduct at an early stage to take advantage of the benefits offered by the Immunity and Leniency Programs. Because the first applicants receive the greatest benefit, there are significant incentives to discover and report on conduct before co-conspirators have the chance to do so. Robust corporate compliance programs which include in-person training, question and answer sessions with counsel, and other features can help businesses identify potential violations of the *Act* and take advantage of immunity from prosecution or significantly discounted fines.

Sometimes, employee conduct crosses the line so slowly from legal communications to illegal cartel activity that employees may not recognize what their conduct has become. Sometimes, employees do not appreciate the severe consequences that cartel activity can bring upon themselves and the corporation. By providing employees with that information as well as an opportunity to ask questions or come forward on a confidential basis, compliance programs can meaningfully assist businesses detect potential anticompetitive activity in time to take advantage of the significant benefits of the Immunity and Leniency Programs.

## Penalty Reduction Owing to Compliance Program

At a speech to the Canadian Bar Association's Fall Competition Law Conference,[[14]](#footnote-14) the Commissioner of Competition outlined his vision of "shared compliance" and introduced a draft bulletin on Corporate Compliance Programs. The Commissioner's speech previewed a significant feature of the draft bulletin: the Bureau proposes to reward "credible and effective" corporate compliance programs. Although it is an "incentive program" through which the Bureau may recommend further fine reductions for leniency applicants, the Commissioner cautioned that it does not give businesses a "free pass" simply by putting a compliance program in place. Rather, the Bureau must conclude that the program already in place was "credible and effective". If it does so, the Bureau will recommend a fine reduction in addition to the reduction contemplated in the Leniency Program. Although the amount of any fine sought remains in the discretion of the Public Prosecution Service of Canada ("PPSC"), the Bureau's recommendation is strongly considered.

Publication of the draft bulletin for public comment revealed that the potential benefits for businesses of implementing a "credible and effective" compliance program go beyond the criminal sphere and the Bureau's Leniency Program.[[15]](#footnote-15) The draft bulletin indicates that the Bureau will consider the effectiveness of a corporate compliance program – at the corporation's request – when:

* recommending fine reductions to the PPSC in the context of the Bureau's Leniency Program;
* seeking administrative monetary penalties in the context of the *Act*'s reviewable practice matters;
* determining whether to proceed with criminal charges or seek a civil remedy in circumstances where the *Act* permits either type of proceeding to address the conduct in issue;
* determining whether to prosecute at all where the *Act* or other legislation provide a due diligence defence; and
* considering whether to agree to a consent agreement or other non-contested resolution rather than continuing with litigation.

Importantly, of course, violation of the criminal or reviewable practices provisions of the *Act* does not automatically mean that the compliance program was not "credible and effective". Thus, a corporation whose employees have engaged in cartel activity, like price-fixing or market allocation, might receive more lenient treatment on the basis of a robust compliance program.

The draft bulletin, however, is quick to caution that should management participate in or condone the violation, the Bureau will likely conclude that management's commitment to compliance was not serious and the program was neither credible nor effective. Who will constitute "management" for the purposes of the Bureau's analysis is important, yet unknown. Is a regional vice-president with pricing authority management? What if that VP's criminal conduct remains hidden from the CEO and the board?

Pursuant to section 22.2 of the *Criminal Code,* only the activities of a corporation's "senior officer" can render the corporation a party to the offence.[[16]](#footnote-16) However, it is not clear whether the Bureau would consider "management" in the draft bulletin to be the equivalent of "senior officer". If so, then every corporation accused of price-fixing as a result of conduct by its "senior officer" would be disqualified from a fine reduction on the basis that "management" was not committed to compliance and the offered incentives would never apply.

For the Bureau's incentive policy to have any practical utility, "senior officer" for the purposes the *Criminal Code* and "management" in the draft bulletin cannot be entirely the same. In the author's view, "management" must be evaluated in the context of the corporate accused, but should in most cases be limited to the board, CEO, COO and/or President to ensure that actions of employees with managerial duties or independent pricing authority do not colour what might otherwise be management's strong commitment to compliance.

# Conclusion

We do not mean to suggest that businesses must start investing enormous sums in the name of compliance to avoid the risks and take advantage of the benefits outlined above. Rather, the above demonstrates that numerous considerations should inform a business' decision about the individual value of a compliance program, and, in particular, the justifiable scope. Media reports concerning cases suggest some businesses have been caught flat-footed by one or two employees chatting with their competitors on Bloomberg resulting in massive fines and civil damages claims. No compliance program will immunize a business from liability. Notwithstanding management's best efforts, senior employees may sometimes embroil the business in anticompetitive conduct and work to keep that conduct secret from their employer. However, as many businesses are loath to discover, in most cases the stakes are too high to ignore compliance completely or to give it only lip service. Increasingly, aggressive enforcers the world over are only too willing to investigate and prosecute businesses whose employees have violated antitrust laws.

1. Melanie Aitken is co-chair of the antitrust and competition practice group at Bennett Jones LLP and Managing Principal of the firm’s office in Washington, DC. From 2009 to 2012 she served as Canada's Commissioner of Competition, in charge of the Canadian Competition Bureau. Emrys Davis is a litigation associate and member of the firm's antitrust and competition practice group. The authors thank Daniel Goldgut, a student at Bennett Jones, for his assistance with this paper. [↑](#footnote-ref-1)
2. See for example: <https://www.youtube.com/watch?v=atojWdNVKSk>. [↑](#footnote-ref-2)
3. *Competition Act*, RSC 1985, c C-34 s 16. [↑](#footnote-ref-3)
4. *Ibid*, s 16(1) [emphasis added]. [↑](#footnote-ref-4)
5. *eBay Canada Ltd v Minister of National Revenue,* 2008 FCA 348 at para 48. [↑](#footnote-ref-5)
6. *Ibid* at para 48. [↑](#footnote-ref-6)
7. *eBay Canada Ltd v Minister of National* Revenue, 2007 FC 930 at para 23. [↑](#footnote-ref-7)
8. *R v Edwards,* [1999] OJ No 3819 at para 89. [↑](#footnote-ref-8)
9. 2013 SCC 60 at para 23. [↑](#footnote-ref-9)
10. Casey W. Halladay & Joshua Chad, A Database too far? Interpreting the Competition Bureau's Computer Search Powers", 2014 *Canadian Competition Law Review* 453. [↑](#footnote-ref-10)
11. Memorandum of Judge Conner dated February 26, 2014 *In re Chocolate Confectionary Antitrust Litigation*, 1:08-MDL-1935. [↑](#footnote-ref-11)
12. *Imperial Oil v Jacques*, 2014 SCC 66. [↑](#footnote-ref-12)
13. *Ibid* at para 87. [↑](#footnote-ref-13)
14. Remarks by John Pecman, Commissioner of Competition, CBA Competition Law Fall Conference, Ottawa Convention Centre, Ottawa, ON: <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03815.html>. [↑](#footnote-ref-14)
15. Corporate Compliance Programs, Bulletin Draft for Public Consultation, <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03778.html#section5> [↑](#footnote-ref-15)
16. *Criminal Code*, RSC, 1985, c C-46 s 22.2. [↑](#footnote-ref-16)