Information Sharing and the 'Reasonable' Ambiguities of s.8 of the Charter

Lisa M. Austin

Version	Post-print/accepted manuscript

Citation (published version)	Lisa Austin, "Information Sharing and the 'Reasonable' Ambiguities of s.8 of the Charter" (2007) 57 University of Toronto Law Journal 499.

Publisher's Statement	Lisa Austin, "Information Sharing and the 'Reasonable' Ambiguities of s.8 of the Charter" (2007) 57 University of Toronto Law Journal 499. Reprinted by permission of the University of Toronto Law Journal
https://doi.org/10.1353/tlj.2007.0006

How to cite TSpace items

Always cite the published version, so the author(s) will receive recognition through services that track citation counts, e.g. Scopus. If you need to cite the page number of the author manuscript from TSpace because you cannot access the published version, then cite the TSpace version in addition to the published version using the permanent URI (handle) found on the record page.

This article was made openly accessible by U of T Faculty. Please tell us how this access benefits you. Your story matters.
Information Sharing and the “Reasonable” Ambiguities of s.8 of the Charter
Lisa M. Austin
University of Toronto Faculty of Law

1. Introduction

In Hunter v. Southam, the first Supreme Court of Canada case to interpret s.8 of the Charter, the court liberated the guarantee against unreasonable search or seizure from its common law roots—indeed shackles—of property. Section 8, wrote Justice Dickson, protects “people, not places” and the interest at stake is privacy, not property.1 This firmly set s.8 within a framework suitable for the modern world where the paradigm for unjustified state intrusions into individual lives is not the knock of the king’s messengers at one’s door. The question is whether the analytical framework outlined by Justice Dickson, and subsequently refined in the Supreme Court’s s.8 jurisprudence, is robust enough to address the privacy challenges of the 21st century, where the major concern is the destruction of informational privacy. To many observers, it is not clear that many traditional privacy paradigms—often focusing on direct state surveillance or the protection of secrecy—can capture what is at stake in emerging practices that create “digital dossiers” on individuals and potentially subject them to forms of “dataveillance.”2 Instead of involving a single state agency in directly collecting personal information that is otherwise shielded from others, these practices often involve a state agency gaining access to information that is already in the hands of third parties—such as those in the private sector or the state in its regulatory capacity. In this way, information-sharing practices are at the center of the debate regarding informational privacy. This paper argues that the Supreme Court’s s.8 jurisprudence has the resources to address the phenomenon of information sharing but in order to do so must adopt greater analytic clarity and rigour in its approach to s.8.

In telling this story, Justice Iacobucci is a perhaps surprisingly central figure. Surprising because, compared to many other areas of the law discussed in this volume, his voice was rarely heard with respect to privacy issues. He wrote very few s.8 decisions during his judicial career and generally concurred with the majority. Nonetheless, he co-wrote two of the most important cases to touch upon s.8 and information sharing: R. v. Mills and R. v. Jarvis.3

---

Mills, co-written with Justice McLachlin, as she then was, contains a statement as important for creating a modern privacy jurisprudence as Hunter’s affirmation that s.8 protects people, not places: “Privacy is not an all or nothing right.” This statement, and its elaboration by Justices Iacobucci and McLachlin, creates the jurisprudential foundation for overcoming one of the most important conceptual hurdles with respect to informational privacy in the context of information sharing. The hurdle results from the fact that in such contexts the initial collection of the information is usually non-problematic and even consented to. If there is nothing amiss in the original collection, then why would there be a problem with the subsequent sharing of this information? In order to argue that information privacy concerns are still present, we need to be able to conceive of privacy as something that is not lost, or strongly diminished, simply because information is shared with others in some contexts for some purposes. Mills affirms that privacy is not lost simply because information is shared and therefore secures the possibility of robust constitutional protection of personal information in the hands of third parties.

However, the legacy of this decision with respect to informational privacy is still uncertain and unfolding. Justice Iacobucci’s later decision, with Justice Major, in Jarvis appears to be in tension with a strong reading of Mills on this point. Jarvis can be interpreted as suggesting that there is no s.8 impediment to the government using information that it has collected in its regulatory capacity for a subsequent investigative purpose. As such, it appears to narrow the impact of Mills by suggesting that there are few impediments to sharing information gathered in the regulatory context. I will argue that Jarvis is rightly decided but should be interpreted cautiously and in light of the need to avoid perpetuating a number of problematic ambiguities that plague s.8 jurisprudence as a whole. These ambiguities—shifting between descriptive and normative accounts of privacy, conflating threshold and balancing stages of analysis, and undue emphasis on ideas of confidentiality—undermine the promise of the analytic structure originally set out in Hunter. Taken together, these ambiguities could work to discount the privacy interest that is seen to be at stake in the regulatory context and add confusion to the relevance of a variety of factors at issue in the information sharing context. Once problems in the jurisprudence due to these ambiguities are illuminated, and avoided, the framework set out in Mills and Jarvis can be cast in a manner that is internally consistent, analytically rigorous, faithful to the general s.8 jurisprudence, and able to meet the contemporary challenges to information privacy.

---

4 Jarvis, ibid. ¶95. Others suggest a narrower reading. For example, Stanley A. Cohen, in Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril (Markham Ontario: LexisNexis Butterworths, 2005), writes: “The important but narrow point to be observed in these cases appears to be the acceptance of this proposition: if a regulatory/administrative enforcement entity is acting bona fide in the course of its mandated activities and comes across evidence of criminality related to the very matters that it is required to investigate for compliance purposes, it may, without the need for further authorization, validly report and pass along such properly acquired information to the police without the need for a separate statutory authority and without the need for a warrant.” This paper offers a different interpretation of Jarvis and related cases.
The stakes in this issue are high. The private sector collects vast amounts of information about individuals. The government, in administering various regulatory regimes and providing numerous government services, also collects large amounts of information about individuals. Although this information used to exist in separate departmental silos, that era is ending. For example, the demands of e-government are motivating governments of all levels to move towards information systems that provide a common platform for data management and greater interoperability, and which would easily facilitate information sharing. Moreover, these developments exist at time when there are many pressures to access this information, whether in private or public hands, for a variety of purposes unrelated to the context of its original collection. Perhaps the most controversial pressures to access information come from law enforcement and national security agencies that are refining their intelligence techniques in the context of the fight against terror, the fight against organized crime, and the fight against internet crime. All of this points to the need to ensure that there is a constitutional framework that permits a robust definition of informational privacy while providing a rigorous framework with which to balance this interest against legitimate state uses of personal information.

2. The s.8 framework for information sharing

The starting point for s.8 analysis is Hunter, the first Supreme Court of Canada case to deal with the Charter right to be free from unreasonable searches or seizures. Justice Dickson, as he then was, writing for the court, held that a proper understanding of the guarantee of freedom from “unreasonable” search and seizure requires a broad and purposive analysis that goes beyond its common law roots of trespass; it protects privacy, not property. At the same time, Justice Dickson emphasized that [t]he guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by s. 8, whether it is expressed negatively as freedom from "unreasonable" search and seizure, or positively as an entitlement to a "reasonable" expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.

He then argued that this balancing between individual privacy and state interests mandates that, in most circumstances, the following requirements must be met for a constitutionally valid search or seizure: prior authorization by someone capable of acting judicially, with such authorization granted according to a standard of “reasonable and
probable grounds, established upon oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search.”

Taking *Hunter* as a point of departure, subsequent case law has refined this general framework. Three aspects of this refinement are important for the discussion of this paper. First, in determining whether s.8 is engaged at all—thereby necessitating the kind of judicial balancing outlined in *Hunter*—the Court has sought to define both search and seizure in terms of whether state action invades a reasonable expectation of privacy. \(^8\) In this way, the idea of “reasonable expectation of privacy” has come to play two roles in the jurisprudence: first, as a threshold test for engaging s.8; second, as a description of the result of the balancing exercise that seeks to weigh an individual’s privacy interest against the state’s interest in intruding upon this privacy in order to determine what level of protection the individual’s interest merits. Therefore, when the court concludes that state action does not intrude upon a reasonable expectation of privacy, this can either mean that there is no privacy interest at stake or it can mean that the proper balance between state interests and individual privacy has already been struck and no further protections are required.

The second refinement to the *Hunter* framework has been to accept a relaxation of the *Hunter* standards in some contexts. The court has affirmed that where the state interests are different from those discussed in *Hunter*, the outcome of the balancing exercise might be different and a different level of protection warranted. \(^10\) For example, the court has accepted departures from the requirement of prior authorization on a standard of reasonable and probable grounds at borders and in the administrative and regulatory context. \(^11\)

Finally, although *Hunter* suggests that a warrantless search is *prima facie* unreasonable, the Court has found in its third refinement that it will not offend s.8 if there are exigent circumstances or if it is authorized by a reasonable law and carried out in a reasonable manner. \(^12\)

This general framework, and its subsequent development, provides the structure for assessing the constitutionality of various information sharing practices. As stated earlier, one of the biggest obstacles in dealing with information sharing is overcoming the perception that once an individual shares information he or she retains no privacy interest in it. Put in terms of the framework just outlined, the argument is that taking information that is legitimately in the hands of third parties does not constitute a seizure because there is not a sufficient privacy interest in it to engage s.8. As a general argument, this is

---

\(^8\) Ibid. ¶43.
\(^10\) Dickson J. indicated this in *Hunter*, ¶43: “Where the state’s interest is not simply law enforcement as, for instance, where state security is involved, or where the individual’s interest is not simply his expectation of privacy as, for instance, when the search threatens his bodily integrity, the relevant standard might well be a different one.”
\(^12\) See, for e.g., *R. v. Collins*, [1987] 1 S.C.R. 265.
inconsistent with the very strong statement of Justices Iacobucci and McLachlin, as she then was, in *Mills*:

Privacy is not an all or nothing right. It does not follow from the fact that the Crown has possession of the records that any reasonable expectation of privacy disappears. Privacy interests in modern society include the reasonable expectation that private information will remain confidential to the persons to whom and restricted to the purposes for which it was divulged. Where private information is disclosed to individuals outside of those to whom, or for purposes other than for which, it was originally divulged, the person to whom the information pertains may still hold a reasonable expectation of privacy in this information.\(^\text{13}\)

Whether a privacy interest remains depends, therefore, on the circumstances in which the individual divulges information to a third party.

The question raised by *Jarvis* is whether it narrows the understanding of privacy outlined in *Mills* so that it does not apply to information collected and held by the state in its regulatory capacity. The implication would be that such information could be shared for law enforcement purposes without any level of constitutionally mandated protection, whether that be the *Hunter* standards or some lesser standard.

However, interpreting the privacy implications of *Jarvis* is difficult because the case was more centrally concerned with s.7 than s.8 of the *Charter*. The issue in *Jarvis* was whether the use of documents produced under statutory compulsion violate the accused’s s.7 protection against self-incrimination. More specifically, the question was whether information legitimately gathered by an auditor pursuant to the inspection and requirement provisions of the *Income Tax Act* could be entered into evidence in tax evasion proceedings. Justices Iacobucci and Major held that the s.7 right against self-incrimination does not attach to validly obtained audit information. However, when the predominant purpose of an inquiry is the determination of penal liability, rather than the administrative function of determining tax liability, then s.7 is engaged and CCRA officials cannot use the inspection and requirement provisions to further their penal investigation. Instead, they must seek warrants in order to gain access to further documents.

Justices Iacobucci and Major also held that there is no s.8 impediment to an auditor passing along information legitimately collected during an audit to CCRA investigators. However, their s.8 reasons are very compressed:

With respect to the consequences related to s.8 of the *Charter*, *McKinlay Transport, supra*, makes it clear that taxpayers have very little privacy interest in the materials and records that they are obliged to keep under the ITA, and that they are obliged to produce during an audit. Moreover, once an auditor has inspected or required a given document under ss. 231.1(1) and 231.2(1), the taxpayer cannot truly be said to have a reasonable expectation that the auditor will guard its confidentiality. It is well known, as Laskin C.J. stated in *Smerchanski, supra*, at p. 32, that “[t]he threat of prosecution underlies every tax return if a false statement is knowingly made in it”. It follows that there is nothing

\(^{13}\) *Mills*, supra note 3, ¶108, citations removed.
preventing auditors from passing to investigators their files containing validly obtained audit materials.\footnote{14 Jarvis, supra note 3, ¶95.}

Therefore even though \textit{Jarvis} would limit information sharing—and its collection using the inspection and requirement provisions of the \textit{ITA}—once the predominant purpose of an investigation is to determine criminal liability rather than tax liability, this is a line that is drawn by s.7 and not s.8.

There are two ways to understand \textit{Jarvis}. The first is to see that the information sharing does not violate a reasonable expectation of privacy because, as a threshold matter, there is not a sufficient privacy interest in the information at issue. In other words, there is no seizure. The second is to see that the information sharing does not violate a reasonable expectation of privacy because the right balance has been struck between state interests and individual privacy in this particular context. In other words, there is a seizure but it is a reasonable one. This paper argues that the second interpretation should be embraced. The following sections outline in more detail what such an analytical framework would entail, in terms of both our understanding of specific cases such as \textit{Jarvis} as well as our understanding of the s.8 jurisprudence as a whole. Such an approach renders \textit{Jarvis} most consistent with previous decisions of Justice Iacobucci, such as \textit{Mills}, as well as avoids the ambiguities that plague s.8 jurisprudence and threaten to undermine its ability to respond to the challenges facing informational privacy.

\section*{3. Privacy, the Regulatory Context, and the Three Ambiguities of s.8}

One way of rendering \textit{Mills} and \textit{Jarvis} consistent is to argue that, in \textit{Jarvis}, the dominant reason for finding that the information sharing did not violate a reasonable expectation of privacy was not because this information was already in the hands of a third party but rather because individuals have a lower expectation of privacy in the regulatory context. As outlined above, in \textit{Jarvis} Justices Iacobucci and Major indicate that the privacy interest of taxpayers in the materials and records produced during an audit under the \textit{ITA} is “minimal.”\footnote{15 McKinlay Transport, supra note 11, is cited for this proposition although even in that case this “minimal” interest was sufficient to render the demand of information a “seizure” thereby engaging s.8. Moreover, \textit{McKinlay Transport} concerned a corporation. The information at issue in \textit{Jarvis} included information about Mr. Jarvis’ farming operations, his deceased wife’s artwork, and his own banking arrangements, all of which could be argued to raise more significant privacy interests than corporate records.} Indeed, the Supreme Court has frequently held that individuals have a \textit{diminished} expectation of privacy in the regulatory context as compared to other contexts.\footnote{16 Thomson Newspapers Ltd. \textit{v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)}, [1990] 1 S.C.R. 425 [Thomson Newspapers]; McKinlay Transport, supra note 11.} The implications of this line of reasoning are that there should be few impediments to the state’s use of information gathered in the regulatory context for other purposes because that information raises minimal privacy concerns.

However, this section examines—and contests—the claim for a lower expectation of privacy in a regulatory context. It locates the reasons for this claim in several ambiguities
in the jurisprudence which, taken together, undermine our understanding of the privacy interests at stake in regulatory contexts. These ambiguities exist within s.8 jurisprudence generally, even if they do particular damage to privacy interests within the regulatory context. They fall into three categories relevant to informational privacy. First, the court shifts between a descriptive and a normative approach to defining privacy. Second, its descriptive approach often conflates the threshold question of defining privacy with the subsequent question of balancing privacy with other important social goals. Third, some of the more normative elements that do provide content to the reasonable expectation of privacy are norms of confidentiality, which, although related, are not the same thing as norms of privacy. The following sections outline these ambiguities in some detail and show how they operate to discount privacy within the regulatory context but in a manner that is particularly problematic if applied without regard to the issues arising from information sharing.

(a) descriptive vs. normative accounts of privacy

Many of the early s.8 decisions of the Supreme Court that sought to provide more content to the privacy interest at the threshold stage of analysis did so through a heavy emphasis on “expectation” in the “reasonable expectation of privacy” test. This resulted in an approach to privacy that can be labelled the “what did you expect?” approach. Such an approach encourages a descriptive account of privacy norms, for what people “expect” is determined through reference to existing social practices. For examples, if an existing social practice is that people do not read through a notebook that has the word “private diary” printed on its cover, then an individual “expects” that his or her private diary will not be read by others. This “expectation” can be given content, therefore, without any more normative enquiry into why private diaries should be protected from the prying eyes of others, including the state. The constitutional entitlement that follows from such an approach would appear to have more to do with protecting settled expectations than with protecting expectations of privacy. It protects an interest in being unfairly surprised by state intrusions but is unable to articulate expected, but nonetheless problematic, invasions of privacy.

An example of this kind of “what did you expect” approach to s.8 can be found in Chief Justice Lamer’s dissenting opinion in R. v. Wong. The case concerned the warrantless use of video surveillance of a hotel room gambling exercise. In arguing that there was no breach of a reasonable expectation of privacy in the case, Lamer C.J. pointed to the fact that the accused had invited the general public to the hotel room. He argued:

A reasonable person would know that when such an invitation is extended to the public at large, one can no longer expect that strangers, including the police, will

---

18 R v. Wong, [1990] 3 S.C.R. 36. Lamer C.J. heard the appeal as a Puisne Judge but was appointed as Chief Justice prior to the release of the decision.
not be present in the room. In this case, the police effected their presence in the room via the video camera which was installed in the drapery valence.\(^{19}\)

The salient question, on this approach, is whether one can reasonably predict that others, including the police, could be present. If the answer is yes, then there is no reasonable expectation of privacy. In this way, it is more of a descriptive inquiry into social practices and understandings than a normative analysis of the purpose of s.8 protection of privacy.

However, s.8 jurisprudence also has many examples of a more normative approach to privacy, thereby relying more heavily on the idea of “privacy” than on “expectation” in the “reasonable expectation of privacy” test. Instead of pointing to social practices, such an approach focuses on the purpose of privacy in fostering important values. This approach, championed in the early jurisprudence by Justice La Forest, would approach the question of video surveillance by asking: even if it is reasonable to expect to be watched (i.e. this is predictable), is this a reasonable practice? Answering this, Justice La Forest argued for the majority in *Wong*, requires an appeal to the values of a free and democratic society. Courts must “assess whether giving their sanction to the particular form of unauthorized surveillance in question would see the amount of privacy and freedom remaining to citizens diminished to a compass inconsistent with the aims of a free and open society.”\(^{20}\)

The Court has recently endorsed this approach in *Tessling*, another surveillance case.\(^{21}\) *Tessling* concerned the warrantless use of Forward Looking Infra-Red (FLIR) technology to record images of thermal energy emanating from the home of the accused. Justice Binnie, for a unanimous court, affirmed that “[e]xpectation of privacy is a normative rather than a descriptive standard.”\(^{22}\) Otherwise, in a context with proliferating means of snooping, individuals could very well “expect” surveillance in contexts that should nonetheless attract s.8 protection.

Other cases have tried to provide more content to this connection between privacy and a free and democratic society. For example, Justices Iacobucci and McLachlin, as she then was, in *Mills* point to the connection between privacy and “many fundamental human relations” as well as to the values of individual “dignity, integrity and autonomy”.\(^{23}\) Instead of a descriptive approach, therefore, these cases point to a purposive inquiry that would answer the question of “reasonable expectation of privacy” by looking to the connection between the privacy interest being claimed and the underlying reasons for constitutional protection of privacy. In the context of informational privacy, this encourages an approach that emphasizes the nature of the information at issue and not social practices concerning that information. For example, in *Mills* Justices Iacobucci and McLachlin argue that when considering information, “privacy concerns are at their

---

19 Ibid. at 63.
20 Ibid. at 46.
21 *R. v. Tessling*, [2004] SCC 67 [*Tessling*]. It was also the last s.8 case that Justice Iacobucci sat on, although he did not take part in the judgment.
22 Ibid. ¶42.
23 *Mills*, supra note 3 ¶81.
strongest where aspects of one’s individual identity are at stake, such as in the context of information ‘about one’s lifestyle, intimate relations or political or religious opinions.’”

This understanding of privacy as a normative and not a descriptive inquiry needs to influence our reading of some of the cases dealing with the reasonable expectation of privacy in a regulatory context. For example, in *B.C. Securities Commission v. Branch*, Justices Iacobucci and Sopinka—writing for the majority—confirmed that that regulatory or administrative searches and seizures require “a less strenuous approach” than the standard appropriate in the criminal context, as outlined in *Hunter*. The main reason offered for a relaxation of this approach in the regulatory context is that there is a diminished expectation of privacy in such contexts. This has two aspects. The first is that because of the nature of regulation which demands the filing of various documents, government intrusion can be “confidently predicted” so as to diminish any expectation of privacy. Second, even where this is not the case, state officials are often given the broad discretion to engage in unannounced inspections so as to induce compliance with the regulatory regime. This can “create in the regulatee an expectation that he may be inspected or requested to provide information at some point in the future.” In the specific regulatory context of trading securities, “[i]t is widely known and accepted that the industry is well regulated. Similarly, it is well known why the industry is so regulated.” On its surface, this case seems to endorse a “what did you expect” approach to defining privacy—in the regulatory context, inspection is utterly predicable and so there is no expectation of privacy. At the same time, the reasoning risks circularity: subsequent state intrusions are reasonable because you do not have much of an expectation of privacy and you do not have much of an expectation of privacy because of the existence of previous state intrusions.

Nonetheless, in light of subsequent cases endorsing a more normative approach to privacy, *B.C. Securities* can, and should, be given another interpretation. Justices Iacobucci and Sopinka, in concluding that the privacy interest at stake is “limited” in fact do outline many of the features salient to a more normative analysis. As they point out, business records have a lesser privacy interest attached to them than personal records. Quoting Justice La Forest in *Thomson Newspapers*, they affirm:

> The ultimate justification for a constitutional guarantee of the right to privacy is our belief, consistent with so many of our legal and political traditions, that it is for the individual to determine the manner in which he or she will order his or her private life. … But where the possibility of such intervention is confined to business records and documents, the situation is entirely different. These records and documents do not normally contain information about one’s lifestyle, intimate relations or political or religious opinions. They do not, in short, deal with those aspects of individual identity which the right to privacy is

---


25 *B.C. Securities*, ibid. The court held that the seizure of documents authorized by s. 128(1) of B.C.’s *Securities Act* does not violate s.8 of the *Charter*.

26 Ibid. ¶52.

27 Ibid. ¶53.

28 Ibid. ¶58.
intended to protect from the overbearing influence of the state. On the contrary, as already mentioned, it is imperative that the state have power to regulate business and the market both for economic reasons and for the protection of the individual against private power. Given this, state demands concerning the activities and internal operations of business have becomes a regular and predictable part of doing business. Under these circumstances, I cannot see how there would be very high expectation of privacy in respect of records and documents in which this information is contained.\footnote{Ibid. ¶62, citing Thomson Newspapers at 517-18.}

Although in this quote Justice La Forest reiterates the idea of what you can predict as being a part of the “expectation” of privacy, the preceding part of his statement is quite helpful for outlining a more normative sense of why business records might have a more limited privacy interest than personal records. Simply put, business records do not engage the purpose of s.8 as directly as personal papers do. In other words, the difference between business papers and personal papers is not marked by the predictability of state intrusion so much as by the degree of connection with the underlying rationale for the constitutional protection of privacy. But this will not be the case with respect to all information that is collected by the state in its regulatory capacity.

In sum, the best approach to providing the reasonable expectation of privacy with content is to focus on the nature of the information at issue and its connection to the underlying values protected by privacy. The “what did you expect?” approach, in focusing on “expectations” tends to lapse into a descriptive rather than normative analysis, emphasizing the predictability of state intrusions and obscuring the value of privacy.

However, in order to shift to a normative approach in the manner just outlined, the jurisprudence must overcome two further difficulties. There are two ways in which the “what did you expect?” approach could take a more normative turn, but both are problematic. The first is through having our understanding of reasonable expectations informed by justifiable societal or state interests. The second is through having this understanding informed by the norms of confidential information. The following two sections outline these approaches and show why they are so problematic for the protection of informational privacy.

(b) conflation of threshold and balancing

Because the language of “reasonable expectation of privacy” is used to both describe the balancing exercise outlined in Hunter, as well as to determine the threshold question of whether something is a search or seizure, the court often conflates these two distinct inquiries. When conflated, factors that relate to the state or societal interest in getting access to information can discount the privacy interest at stake. In other words, society’s interests play a role in determining whether there is a search as well as whether that search is “reasonable” for the purposes of s.8. Indeed, in Tessling, the court goes so far as to suggest that this balancing does in fact inform both the question of whether there is a
search as well as whether the search is reasonable. This is problematic because it risks having societal interests double-count: once in order to diminish the privacy interest that is seen to be at stake and again in order to justify state intrusion upon that diminished privacy interest.

Such double-counting of societal interests also operates in the privacy jurisprudence regarding the regulatory context. For example, it is at play in the reasons of Justices Iacobucci and Sopinka in *B.C. Securities*. As outlined in the previous section, they first find a “limited” privacy interest at stake in the regulatory context. They then go on to argue that “[i]n this case, the outstanding issue is whether the law is reasonable”. This is a reference to the analysis that is applicable to the balancing stage. In the absence of prior authorization, for a search or seizure to be reasonable it must be authorized by law, the law must be reasonable, and the manner of search must be reasonable. When answering the question of whether s.128(1) of the *Securities Act* is “reasonable” in this sense, they answer yes. However, importantly, they do so through reference to the considerations that in other parts of the judgment factored into their answer to the threshold question: “We have already mentioned that in a highly regulated industry, such as the securities market, the individual is aware, and accepts, justifiable state intrusions.” The important point here is not that state intrusions are expected but that they are justifiable. In other words, another way to argue why the administrative context accepts a relaxation of the *Hunter* criteria is because of the importance of ensuring the effectiveness of compliance in relation to an important regulatory regime. It is a question of balancing state interests with individual privacy and not discounting the privacy interest from the outset—particularly when that discounting occurs through advertence to the very same state interests that it is later balanced against.

Double counting can unduly diminish the privacy interest seen to be at stake in a particular situation. But conflation of threshold and balancing can do further damage to informational privacy in the context of information sharing. An example can make this clearer. The Canadian judicial system considers most court documents to be “public.” The reason for this is not that these documents lack privacy concerns: often these documents include highly private information pertaining to individuals’ finances, mental and physical health, and family circumstances. The “public” nature of these documents refers to the fact that the public’s interest in getting access to these documents generally outweighs the privacy interests at stake. This public interest is the open courts principle: public access fosters accountability in the judicial system. However, not all subsequent uses of these records will engage this same justification. For example, commercial data mining of court records has little, if anything, to do with the principle of open courts and

---

30 *Tessling*, supra note 21, ¶17-18. There is some limited recognition of this problem in the Supreme Court jurisprudence. For example, in *Tessling* Binnie J. argues that *Plant* factors such as the “seriousness of the offence” go to the question of balance rather than threshold although he retains a consideration of the intrusiveness of the search in the threshold analysis—which looks to be more properly a kind of proportionality analysis better suited to the balancing analysis. Ibid. ¶42 and ¶64.

31 *B.C. Securities*, supra note 24 ¶61.

32 Ibid. ¶64.

33 There are, of course, legal procedures to seal records.
there is no reason to think that court records need to be made available for this purpose.\footnote{34} In order to conceive of some of these uses as intrusions upon privacy, the determination of the nature of the privacy interest and the balancing of this against societal interests must be kept separate. Otherwise, the justificatory factors that may only be present in some contexts operate to discount the individual’s privacy interest in the information generally so that subsequent uses of the information that do not fall within this initial justification cannot even be properly conceived of as intrusions upon privacy.

\textbf{(c) privacy vs. confidentiality}

Another way in which the “What did you expect?” approach takes on normative dimensions is through reference to the norms of confidentiality.\footnote{35} Indeed, when the Supreme Court discusses privacy, it often uses privacy and confidentiality as interchangeable terms. Such a move, however, raises important questions when considering the permissibility of information sharing as it can in fact unduly narrow the protection afforded to informational privacy.

I would like to sharpen the distinction between privacy and confidentiality through reference to some recent case law regarding the common law of privacy and the common law of breach of confidentiality. The classic statement of breach of confidence is found in \textit{Coco v. AN Clark (Engineers) Ltd}, where Justice Megarry, as he then was, identified three elements for a successful breach of confidence claim:

\begin{enumerate}
  \item the information must have the necessary quality of confidence about it;
  \item the information must have been imparted in circumstances importing an obligation of confidence; and
  \item there must be an unauthorized use or disclosure of that information to the detriment of the party communicating it.
\end{enumerate}

The first two elements are particularly important in the context of the present discussion. With respect to the first element, the “necessary quality of confidence” refers to the fact that the information is kept secret rather than any more intrinsic quality to the information itself.\footnote{37} The second element has traditionally focused on the relationship between the party who discloses the information and the party who is in receipt of the information, thereby restricting the protection afforded to the information.

\footnote{34} The Canadian Judicial Council has recently adopted a model policy regarding access to court records stating that “if court records are accessed and utilized for improper purposes or in a manner that subverts justice, then public confidence in the administration of justice might be undermined” and recommends that bulk access be governed by special agreement with the court. See Canadian Judicial Council, \textit{Model Policy for Access to Court Records} (2006), online: Canadian Judicial Council <\url{http://www.cjc-ccm.gc.ca/article.asp?id=2985}] at ss. 1.1 and 5.2.

\footnote{35} Similarly, when discussing spatial privacy, the Supreme Court invokes norms of property. See, for e.g. \textit{R. v. Edwards}, [1996] 1 S.C.R. 128, \textit{Tessling supra note 21}.


\footnote{37} Lord Greene M.R. stated in \textit{Saltman Engineering}, “[t]he information, to be confidential, must, I apprehend, apart from contract, have the necessary quality of confidence about it, namely it must not be something which is public property and public knowledge.” \textit{Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd.} (1948) 65 R.P.C. 203 at 215.
highlighting the roots of breach of confidentiality as an equitable doctrine applicable to relationships of confidence and trust.

From this classic point of departure, the breach of confidentiality action has been undergoing a rapid transformation, particularly in the UK. There no longer needs to be a relationship of confidence where the information in question is “obviously confidential.”\(^{38}\) Under the influence of European human rights law, this has further developed, in cases such as \textit{Campbell},\(^{39}\) to catch information that is “private” where private is understood to designate something about the nature of the information protected beyond the fact that it is “not public.” Arguably, this has made breach of confidentiality in the UK more like an action for the invasion of privacy in other jurisdictions.\(^{40}\)

While this shift highlights the close connection between privacy and confidentiality, it also points to important distinctions: it is the idea of privacy that brings with it a focus on the nature of the information itself and its connection to the fostering of certain values whereas confidentiality is traditionally concerned with protecting certain kinds of relationships and it is only important that the information protected not be public. Privacy can therefore be broader than confidentiality, in that it does not rely upon the existence of a confidential relationship, and because it is not inherently contradictory to say that there are privacy interests in information that is open to public view.\(^{41}\) At the same time, privacy can be narrower than confidentiality: apart from the non-public element, there is no limit on the type of information that can be considered confidential, and confidential information can encompass a wide variety of business documents that have little or no connection to fostering values such as the autonomy and dignity of individuals in their private lives.\(^{42}\)

There is nothing wrong with holding that s.8 protects information that is either private or confidential. It would be regrettable, however, if the Court conclusively imported some of the criteria applicable to confidentiality in order to reduce the scope of s.8 protection to information that is both private and confidential. The potential effect of this in the context

\(^{38}\) \textit{Attorney-General v. Guardian Newspapers Ltd.} (No. 2), [1990] 1 AC109 at 281 per Lord Goff.

\(^{39}\) \textit{Campbell v. MGN Limited} [2005] UKHL 61.

\(^{40}\) Lord Hoffmann in \textit{Campbell}, ibid. ¶51, went the furthest in recognizing this, arguing that, under the influence of human rights law, the “centre of gravity” of the action for breach of confidence has shifted to focus “upon the protection of human autonomy and dignity-the right to control the dissemination of information about one’s private life and the right to the esteem and respect of other people. The New Zealand Court of Appeal in \textit{Hosking v. Ruting} [2005] 1 NZLR 1 (CA) recognized a tort of invasion of privacy and indicated that the UK action for breach of confidentiality as outlined in \textit{Campbell} was essentially the same.

\(^{41}\) This finds some support in the case law. For example, in \textit{R. v. Mentuck}, [2001] 3 S.C.R., the Supreme Court upheld a publication ban in order to protect privacy even though the public was entitled to be present in the courtroom and so the information at issue was “public” in this sense; it has also recognized privacy interests in one’s movements on public roads (\textit{R. v. Wise}, [1992] 1 S.C.R. 527) and in one’s photo taken in a public place (\textit{Aubry v. Éditions Vice-Versa inc.}, [1998] 1 S.C.R. 591).

\(^{42}\) In \textit{R. v. Law}, [2002] 1 S.C.R. 227, ¶16, the Court tried to the issue of confidential business documents to ideas of privacy, but this shouldn’t be necessary. Even in \textit{Hunter}, supra note 1, ¶ 25, Justice Dickson was careful to indicate that s.8 could protect values other than privacy.
of the permissibility of information sharing would be to narrow the constitutional protection of privacy through an undue focus on the relationship between the individual and the party who holds information about him or her, as well as on the question of whether the information in issue is available to the public in some sense. For example, in Tessling Justice Binnie interprets R. v. Plant, which dealt with the nature of the privacy interest in electricity consumption records, in the following worrisome terms:

It was held that within the commercial relationship of supplier and customer, the accused had knowingly disclosed his electricity consumption to the utility company, with no arrangement as to confidentiality. Such records could be accessed on-line by the police, and thus no reasonable expectations of privacy existed.43

However, in addition to asking whether the information could be considered confidential, Sopinka J. in Plant also asked whether the information could be said to constitute a “biographical core.” By suggesting, as Justice Binnie does in Tessling, that Plant’s conclusion of no reasonable expectation of privacy rested on a lack of confidentiality, the implication is that all information that is in the hands of third parties that does not have an arrangement as to confidentiality is available for perusal by the police without any kind of prior authorization. Such an approach should be rejected: information that is in the hands of third parties should attract s.8 protection if the nature of the information itself demands it. A lack of confidentiality does not mean a lack of privacy.

4. The Significance of Third Parties

According to the arguments of the previous section, the general proposition that individuals have a diminished expectation of privacy in the regulatory context rests upon several serious ambiguities in s.8 jurisprudence: a problematic emphasis on description and prediction; a conflation between determining privacy and balancing this against societal interests; and a confusion between privacy and confidentiality. Instead, in determining an individual’s privacy interest in information, courts should engage in a normative analysis, linking the information to the underlying purposes of the s.8 guarantee. There may be many regulatory contexts in which such an analysis will still result in the finding of a diminished privacy interest but it leaves open a clearer possibility that there will be some regulatory contexts in which informational privacy interests remain strong.

Even if the information, when originally collected, is considered private, one could still argue that once it is justifiably in the hands of a third party, including the state, no privacy in the information remains. On its face, Justices Iacobucci and Major appear to endorse this approach when, in Jarvis, they assert that once the auditor has the information, the taxpayer no longer has any reasonable expectation as to its confidentiality. However, as a general statement, this is inconsistent with Justices Iacobucci and McLachlin’s very strong language to the contrary in Mills, as already outlined.

43 Tessling, supra note 21, ¶60.
Nonetheless, there are other ways in which to cast the significance of third parties. For example, even if one accepts that a privacy interest remains in relation to the state, one could argue that s.8 does not prevent the third party from itself voluntarily sharing the information with the state. That is, if a third party has obtained information in a permissible manner, then it is free to pass this along to law enforcement agents on its own initiative. The only s.8 concern, on this view, is when law enforcement agents themselves demand the sharing of this information as then they could be said to avoid s.8 requirements by obtaining information that was collected under a regime that attracted a lower—or even no—level of constitutional protection. That is, we should not permit law enforcement agents to do indirectly what they cannot do directly, absent special authorization such as a warrant or specific legislation.

However, the Supreme Court’s s.8 jurisprudence indicates that the line between constitutionally permissible and impermissible information sharing is not the line between voluntary and involuntary information sharing. This is clear from R. v. Dyment, a case decided before Justice Iacobucci’s appointment to the Court.\(^{44}\) The accused in Dyment was charged with impaired driving and sought to exclude evidence of blood analysis on the ground that the taking of his blood sample amounted to an unlawful seizure in violation of his s.8 rights under the Charter. The blood was originally taken from the accused by his physician for medical purposes and there was no issue with respect to this original collection.\(^{45}\) After the patient subsequently told the physician that he had consumed a beer and some antihistamines, the physician handed Mr. Dyment’s blood sample to the police who charged him impaired driving.

The case turned on the question of whether this voluntary sharing of the blood sample amounted to a seizure.\(^{46}\) Justice LaForest, writing for the majority on this question, held: “[i]f I were to draw the line between a seizure and a mere finding of evidence, I would draw it logically and purposefully at the point at which it can reasonably be said that the individual had ceased to have a privacy interest in the subject-matter allegedly seized.”\(^{47}\) The central issue, therefore, is not whether the police actively sought the evidence or merely received it. In other words, the question does not turn on the actions of the police—although the nature of these actions could certainly bolster the finding of a seizure—but rather on the nature of the individual’s privacy interest in the thing seized. On the facts of Dyment, the question was whether Mr. Dyment, once the doctor validly

\(^{44}\) Dyment, supra note 9.

\(^{45}\) Ibid. The patient had been bleeding and unconscious at the time as a result of a car accident. Although the patient had not consented to the original collection of the blood, because the physician took it for medical purposes, thinking that the accident might have been caused by some kind of medical condition, there was no issue with respect to the impropriety of the original collection.

\(^{46}\) However, LaForest J. stated: “though we have no evidence to indicate the nature of the “conversation” between the doctor and the officer, I find it hard to believe the doctor merely volunteered it.” However, his decision did not turn on this. Ibid., ¶30.

\(^{47}\) Ibid. ¶30. This is also consistent with what the Court has held with respect to what constitutes a search. As the Court recently affirmed in Tessling, government actions constitutes a search “only where … state examinations constitute an intrusion upon some reasonable privacy interest of individuals.” Tessling, supra note 21, ¶18.

\(^{48}\) See, for e.g., R. v. Poheretsky, [1987] 1 S.C.R. 945, where the police requested that the doctor obtain a blood sample from a delirious patient.
obtained the blood sample, continued to have a privacy interest in that sample vis-à-vis the state. The answer was clearly yes, as the physician who took the blood sample was understood to hold it “subject to a duty to respect the dignity and privacy of that person.” Therefore if an individual has a reasonable privacy interest in information in the hands of third parties, then the sharing of this information with the state engages s.8 regardless of whether the state actively seeks this information or merely “receives” it. The important element is not the nature of the actions of the police, but the effect of the information sharing on the individual. Justice Iacobucci underscores this general point in his dissent in Schreiber where he states that “[t]he focus of the right to privacy … is the impact of an unreasonable search or seizure on the individual.”

The final possibility for the significance of third parties is the “scope of duties” rationale that follows from the Supreme Court’s decision in Colarusso and its subsequent interpretation in Laroche, two important information-sharing cases in which Justice Iacobucci concurred with the majority opinions. This rationale would hold that when the third party is an administrative agent acting within the scope of his or her duties, then passing information along for the purposes of a criminal investigation does not require any further statutory authorization or a warrant. However, I argue that although the fact that a third party was acting within the scope of his or her duties is significant, its significance does not go to the question of whether there was a seizure but to the question of whether that seizure was reasonable. Moreover, the mere fact that the third party was acting within the scope of his or her duties is not, on its own, sufficient to render the seizure reasonable.

Colarusso concerned the constitutionality of police use of blood and urine samples collected from an individual who had been charged with impaired driving. The accused, Mr. Colarusso, had been driving his car when he lost control and caused an accident, killing another driver. He was arrested at the scene and charged with several offences related to impaired driving. At the hospital, he consented to hospital staff taking blood and urine samples for medical purposes. The coroner requested these samples for analysis to aid him in determining the cause of death, as he is required to do under the Coroner’s Act. The coroner then handed the samples to the police so that they could transport them to the Centre for Forensic Sciences in order to be analyzed. The results of this analysis became crucial to the police case against Mr. Colarusso and his conviction at trial.

Justice La Forest, writing for the majority, held that the police seized the blood and urine samples independently of the coroner’s seizure. He argued that “the officers who transported the blood and urine samples knew of the potential incriminatory nature of the samples and intended to use the results of the analysis for their own purposes at the outset.” Given that this was a seizure of bodily fluids for use in a criminal prosecution, it had to comply with the Hunter requirement of prior authorization. The fact that the coroner exercises his power to seize the samples under the Coroner’s Act does not

---

49 Dyment, supra note 9, ¶28.
diminish Mr. Colarusso’s reasonable expectation of privacy in relation to the use of these samples for criminal law purposes.

In a subsequent case, *Laroche*, the trial judge interpreted *Colarusso* as holding that information collected in the course of an administrative investigation could not be used in the context of a criminal investigation. *Laroche* concerned a number of rebuilt vehicle files. In Quebec, the Société de l’assurance automobile du Québec (SAAQ) issues certificates of technical compliance to rebuilt vehicles that it has inspected and determined meet the manufacturer’s standards. This certificate is mandatory if the vehicle is to be licensed. In the course of an audit, an employee of the SAAQ found a number of serious irregularities in five of the rebuilt vehicle files from Garage Côté Laroche Inc. Convinced that stolen parts had been used to rebuild a number of the vehicles in issue, the employee passed the files to the police.

The Supreme Court of Canada disagreed with the trial judge’s interpretation of *Colarusso*, as did all of the parties upon appeal. Justice LeBel held, for the majority, that the handing over of rebuilt vehicle files that contained suspicious irregularities by an (SAAQ) employee to the police did not violate s.8 of the *Charter*:

Suffice it to note that the SAAQ employee was auditing rebuilt vehicle files submitted by the respondents in order to obtain certificates of technical compliance. The information thus obtained had originally been provided by the respondents, in compliance with the obligations imposed by the legislation and the regulations that applied under the legislation. Laroche and Garage Côté Laroche Inc. should have known that this information would necessarily be examined and audited by the SAAQ and was not, properly speaking, private in relation to the government. In carrying out and expanding his investigation, the employee was merely performing the duties of his position. Transmitting information to the police, to initiate an investigation into the irregularities that had been observed, was connected with the performance of his duties.

Unfortunately, the Court did not outline in any greater detail why it thought that *Colarusso* did not apply but there are at least two major considerations indicated in the reasons: no reasonable expectation of privacy in the information and the employees performance of his duties.

As a threshold matter, there is a plausible argument that there was not a sufficient privacy interest in the information in question to engage s.8. Justice LeBell suggests that this follows from the fact that Laroche should have known that the information provided would be examined and audited by the SAAQ. For the reasons provided in the previous section, a preferable manner of reasoning about the privacy interests at stake in this kind of case would be to argue that the information at issue did not meet the threshold needed to engage s.8 because it was unconnected to the core values of privacy protection. This was clearly business information rather than personal information, and business information that was difficult to say either involved any privacy interest or was confidential.

---

52 Ibid., ¶83-4.
Apart from this, the difference between Colarusso and Laroche is tied to the idea of acting within the scope of one’s duties. The court in Laroche found that transmitting information of irregularities to the police lies within the scope of the duties of the SAAQ. In contrast, the coroner’s passing of the blood and urine samples to the police to be used in connection with a criminal prosecution (although this was not the coroner’s intent) is not a part of the performance of the coroner’s duties in determining whether to hold an inquest.53

But what, precisely, is the significance of the scope of duties? The only way in which the scope of duties can diminish an individual’s privacy interest in the information passed along is if the court adopts a “what did you expect” approach to defining privacy. That is, if the duties of a third party include passing information along to law enforcement agents in some circumstances, then how can you expect to retain privacy in this information in relation to the state? Apart from the problems already discussed in relation to this approach to privacy in general, adopting this line of reasoning here avoids discussion of the most crucial question of all: even if the scope of duties includes passing along information for law enforcement purposes, are these duties reasonable? In other words, the duties themselves should be subjected to constitutional scrutiny. This approach would focus on the balancing stage of s.8 analysis rather than the threshold stage. Assuming that passing the information along constitutes a seizure, the question would be whether this was a reasonable seizure. A warrantless seizure may be reasonable if authorized by a reasonable law and undertaken in a reasonable manner. If actions fall within the scope of duties authorized by a reasonable law, then the seizure could be said to be reasonable without requiring any further authorization. However, the key question would still be the reasonableness of the law and the answer to that question turns on the balance between an individual’s privacy interest and the state interest in that context. In other words, on this approach the scope of duties is an important but not determinate element of the balancing exercise, not the threshold determination, inherent in the reasonable expectation of privacy.

5. Reasonable Seizure

The portion of the analysis where the regulatory context has the most relevance is therefore not at the threshold stage, but at the balancing stage, where individual privacy interests are balanced against state or societal interests in order to determine what level of protection is warranted. Although the compressed s.8 reasons of Jarvis are not explicit in this regard, the best way to interpret the case is in terms of this balancing. Indeed, these considerations are present in the s.8 jurisprudence as a whole but the ambiguities already discussed needlessly confuse the analysis in a manner that has the potential to seriously undermine informational privacy. A better approach, therefore, is to adopt a normative and purposive approach to determining privacy and then explicitly balance this interest against societal interests. Moreover, the jurisprudence should also adopt a more rigorous balancing analysis, explicitly importing many of the types of considerations it already

53 In fact, under the Coroner’s Act a jury at an inquest is forbidden from making any findings of legal responsibility: R.S.O. 1990, c. C.37, s. 31 (2).
uses in its s.1 analysis such as rational connection, minimal impairment and proportionality considerations. This section will outline how such an approach would provide more precision to the *Jarvis* analysis while at the same time indicating more clearly how one could determine whether other types of information sharing practices are constitutionally acceptable.

Assume that the privacy interest attaching to the information at issue in *Jarvis* was higher than the “minimal” interest found by Justices Iacobucci and Major. There are nonetheless many compelling reasons why the passing along of information by the auditor to the investigators constitutes a reasonable seizure of that information. The reasons are essentially the same reasons as why the inspection and requirement powers of the *ITA* are reasonable in the context of an audit, as held in *McKinlay Transport*. According to Justice Wilson in *McKinlay*, the *ITA*’s departures from the *Hunter* criteria are justified not simply by the fact that the *ITA* is regulatory legislation but because of a number of unique features of the scheme itself. Importantly, Justice Wilson pointed out that the *ITA* is based on self-reporting and self-assessment and that it would be too “expensive and cumbersome” to have a different type of scheme. To make such a scheme effective,

> [t]he Minister of National Revenue must be given broad powers in supervising this regulatory scheme to audit taxpayers’ returns and inspect all records which may be relevant to the preparation of these returns. The Minister must be capable of exercising these powers whether or not he has reasonable grounds for believing that a particular taxpayer has breached the Act. Often it will be impossible to determine from the face of the return whether any impropriety has occurred in its preparation. A spot check or a system of random monitoring may be the only way in which the integrity of the tax system can be maintained.54

What is important here is that Justice Wilson, in undertaking the balancing exercise, points to criteria that strongly echo the s.1 *Oakes* criteria of rational connection, minimal impairment and proportionality.55 The ability to audit taxpayer records randomly is not a fishing expedition but is rationally connected to the ability of the Minister to enforce the *ITA*. Moreover, given the fact that there is often no other way to determine whether taxpayer returns were prepared properly, and that a different kind of reporting regime would not work, the audit powers would satisfy a minimal impairment analysis. In addition, Justice Wilson pointed out that the *ITA* protects tax information from most forms of further disclosure of that information.56 As she concludes, the inspection and requirement powers, in the context of an audit, provide “the least intrusive means by which effective monitoring of compliance with the *Income Tax Act* can be effected.”57

With respect to a proportionality analysis, Justice Wilson indicates that the income tax system is the government’s chief source of revenue; maintaining its integrity would justify some intrusions upon taxpayer privacy. Justice Wilson also indicates that in other circumstances, where a taxpayer’s privacy interest might be much stronger—such as when tax officials enter the private property of a taxpayer—then the balancing between state and individual interests might dictate safeguards closer to the *Hunter* requirements.

---

54 *McKinlay Transport*, supra note 11, ¶36.
56 *McKinlay Transport*, supra note 11, ¶38.
57 Ibid., ¶38. Cited in *Jarvis*, supra note 3, ¶65.
It is also likely that in such cases, searches without prior authorization would also fail a minimal impairment or proportionality analysis.

Although Jarvis concerns the constitutionality of the subsequent passing of the information to the CCRA investigators, and not the initial collection of the information, Justices Iacobucci and Major advert to many of the same considerations in their reasons in Jarvis. After reiterating many of the same factors outlined by Justice Wilson, they further argue that “[t]o be effective, self-enforcing regulatory schemes require not only resort to adequate investigation, but also the existence of effective penalties.”\(^{58}\) They also acknowledge that without information obtained through the audit function, it would be difficult for investigators ever to obtain a search warrant because they would have no evidence to support one. As Justices Iacobucci and Major warn, “we should be careful to avoid rendering nugatory the state’s ability to investigate and obtain evidence of these offences.”\(^{59}\)

Why then do these considerations not also justify the use of the inspection and requirement powers in order to further an investigation under the Act, rather than simply to initiate it? There are two reasons. The first is the s.7 concern regarding self-incrimination that formed the central analysis of Jarvis.\(^{60}\) But a second reason can be outlined within the framework of the s.8 analysis just provided. Permitting investigators to have direct recourse to these powers would not satisfy a minimal impairment analysis as such a practice would not be the least intrusive means to achieve the goal of furthering penal investigations.

### 6. Conclusions

This paper has argued that one of the core issues regarding informational privacy in the 21\(^{st}\) century is the issue of information sharing. The question is not whether the state will engage in information sharing practices, or even whether it should. The real question is whether such practices will be subject to constitutional scrutiny and thereby required to meet a rigorous standard of justification. If s.8 jurisprudence continues to exhibit the ambiguities outlined in this paper, then there is a real worry that such practices will attract little constitutional scrutiny, as the courts will find it too easy to hold that such practices do not violate a reasonable expectation of privacy.

The approach advocated in this paper avoids these problems by providing a more structured and coherent framework for s.8 analysis. This approach can be summarized as follows:

1) Whether something is a search or seizure depends upon the existence of a privacy interest of sufficient importance to engage s.8.

\(^{58}\) Jarvis, supra note 3, ¶55.

\(^{59}\) Ibid., ¶90.

\(^{60}\) This reason is not independent of the s.8 argument. In Mills, supra note 3, ¶88, Justices Iacobucci and McLachlin hold that “a reasonable search or seizure is consistent with the principles of fundamental justice.” Therefore if information sharing violates s.7, it also violates s.8.
2) In determining the answer to 1), courts should engage in a normative, purposive analysis regarding the connection between the information in question and the underlying purposes of the s.8 guarantee. Courts should avoid the problems outlined regarding an undue emphasis on the predictability of the intrusions, state or societal interests in access to this information, or norms of confidentiality.

3) If s.8 is engaged, then the individual’s privacy interest needs to be balanced against state interests in accessing the information in order to determine the required level of protection. In undertaking this analysis, courts should structure their reasoning more explicitly by adopting the criteria employed in s.1 analysis under the Charter: rational connection, minimal impairment and proportionality.

There are many remaining questions regarding this framework. For example, the relationship between s.8 and s.1 of the Charter merits further elaboration and is undeveloped in the jurisprudence. Furthermore, a more detailed account of the purpose of the s.8 guarantee would make the purposive analysis advocated easier to implement.61

Nonetheless, the framework for analysis advocated here is consistent with the existing jurisprudence in that applying it does not render past decisions wrongly decided but does reinterpret the significance of some of the relevant factors adverted to by the Court. In this sense, it seeks to make explicit many of the considerations that are already implicit in the jurisprudence and place them within a rigorous framework that permits both a consistent approach to s.8 as well as one able to address contemporary privacy issues. Set within its structure, Justice Iacobucci’s insights in both Mills and Jarvis regarding informational privacy and its justified intrusions can provide the means by which information sharing practices are subject to constitutional scrutiny and intrusions upon privacy held to a high standard of justification.

61 Two of the best examples in the jurisprudence are Justice La Forest reasons in Dyment, supra note 9, and Justices Iacobucci and McLachlin’s reasons in Mills, supra note 3. The purposive approach underlying the s.8 discussion in these decisions contrasts with the more recent Supreme Court decision in Tessling, supra note 21, where in attempting to summarize the jurisprudence, Justice Binnie reproduces most of the ambiguities critiqued in this paper.