The Law Behind Bill C-51

Bill C-51 is now the law. It received Royal Assent on June 18, 2015 with a new name: *Anti-terrorism Act, 2015* and its five parts have been in force and operational since August 1, 2015.

In this paper, I review some of the developments since the bill became law and discuss a small subset of the many legal and *Charter* issues that raised by the bill. The bill was drafted against a backdrop of existing law with a view to test and extend the legal and *Charter* limits of the surveillance state and its security apparatus. The discussion here is not meant to provide an authoritative exposition on the law but rather an overview of some of the issues to hopefully prompt further discussion and to point to possible legal avenues for challenging or mitigating some of the more egregious provisions of the bill.

Political Developments

Despite the change in government, prospects for significant legislative changes to Bill C-51 do not appear to be very good. In opposition, the Liberal government lauded the provisions in the bill that increased preventative arrest, broadened no-fly lists, and enhanced the ability of the national security agencies to access personal information held by the government departments and agencies[1] and supported the passage of the bill. The Liberals campaigned on a promise to provide better oversight of the national security agencies, including the creation of a parliamentary oversight committee modeled on similar committees in the other Five Eyes partners of Canada, but offered no specifics as to other changes.[2] Shortly after the election, the new Liberal government promised a speedy overhaul of the bill with public and expert consultations on proposed changes to the bill as well as the promised parliamentary oversight committee and the repeal of "problematic elements of Bill C-51."[3] Despite some early efforts by Ralph Goodale, the Minister of Public Safety and Emergency Preparedness, to review how the other Five Eyes parliamentary oversight committees work, the Liberal government has not started the public consultation process nor introduced a bill to at least establish a parliamentary oversight committee. In the meantime, it is business as usual for the security agencies and their new enhanced powers granted them by Bill C-51.

Overview of Bill C-51

Bill C-51 is a typical unwieldy Harper government omnibus bill. The Bill combined new laws and amendments in a variety of disparate areas under the umbrella of a response to the threat posed by terrorism to this country. A common theme runs through much of the Bill: access to and dissemination of information. The bill has five parts:

1. The *Security of Canada Information Sharing Act* which is intended to facilitate information sharing among government agencies to counter activities that undermine the security of Canada.

[1] Remarks by Liberal Party of Canada Leader Justin Trudeau on Bill C-51, February 5, 2015
[2] The Five Eyes are Canada, US, UK, New Zealand and Australia.
[3] Rt. Hon. Justin Trudeau, Mandate Letter to the Minister of Public Safety and Emergency Preparedness

2. The *Secure Air Travel Act* which gave legislative bones to the "no fly" list being operated by Transport Canada under the Passenger Protect Program. The information on the list is compiled by the government and distributed to the air carriers for enforcement.
3. Amendments to the *Criminal Code* to, *inter alia*, create a new terrorist propaganda offence[4] and lower the threshold for obtaining a terrorism peace bond to "reasonable grounds that another person may commit a terrorism offence."[5] The new terrorist propaganda provisions are intended to prohibit the dissemination of certain opinions and information.
4. Amendments to the *Canadian Security Intelligence Service Act* to give the Canadian Intelligence Service (CSIS) new powers to take measures to disrupt perceived threats to the security of Canada and to apply to a Federal Court judge for a warrant authorizing CSIS to break the law and violate the *Charter* if necessary to take such measures. These amendments only indirectly address access to information insofar as they provide a means for CSIS with the assistance of the Communications Security Establishment Canada (CSE) to use aggressive measures such as malware to circumvent encryption techniques, a current concern of security agencies around the world.
5. Amendments to the Security Certificate review system under the *Immigration and Refugee Protection Act* to make it easier for the Minister to refuse to disclose sensitive information to the Special Advocate appointed to protect the interest of the person challenging his or her detention under a Security Certificate. Here the purpose is to limit and deny access to information that may arguable assist a person subject to a Security Certificate in challenging the Minister's decision.

Security of Canada Information Sharing Act (SCISA)[6]

The *Security of Canada Information Sharing Act* (*SCISA*) creates a new legal regime to give the 17 government agencies designated under the Act virtually unfettered access to personal information held by any government agency, regardless of the original purpose for the collection or obtaining of the personal information. The information sharing regime is apparently fully operational although government officials to date have provided no information on the volume or scope of the access to or use or disclosure of personal information by the securities agencies under the *Act*.

The central provision of the Act is Section 5(1) which authorizes any of the 100+ Government of Canada institutions to disclose information to one of the 17 government agencies designated under the Act "if the information is relevant to the recipient institution's jurisdiction or responsibilities under an Act of Parliament or another lawful authority in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption."

Section 5(1) has the effect of removing the restrictions on the use and distribution of personal information created by the *Privacy Act*. In general, a government institution can only use or disclose personal information for the purpose for which it was originally collected or obtained or for a use which

[4] Section 83.221, Advocating or Promoting Commission of Terrorism Offences
[5] Section 810.011, Fear of Terrorism Offence
[6] In force August 1, 2015: SI/2015-0064.

is consistent with that purpose.[7] However Section 8 (2)(b) of the *Privacy Act* permits the disclosure of personal information "for any purpose in accordance with any act of Parliament … that authorizes its disclosure."[8] Section 5(1) of the *SCISA* is clearly intended to authorize such disclosure and acts as a broad exemption from the privacy protections in the *Privacy Act.* The Privacy Commissioner of Canada noted this effect in his letter to the House Committee considering Bill C-51: "if adopted in its current form, the *Security of Canada Information Sharing Act* would make available to 17 federal departments and agencies, which hold some responsibilities in relation to national security, potentially all personal information that any department may hold on Canadians."

The relevancy standard used in Section 5(1) sets a minimal legal threshold, below that of reasonable grounds, balance of probabilities or reasonable suspicion in the context of search and seizure and below the true relevancy and obviously or likely relevant thresholds required for access to third party records. In the trial context, relevance is broadly construed: "[e]vidence is logically relevant where it has any tendency to prove or disprove a fact in issue."[9] The test of relevancy under Section 5(1) is even lower: the information need only be relevant to the agency's responsibilities to detect, identify, analyze, prevent, investigate or disrupt activities that undermine the security of Canada. More simply the information need only be of potential use to the agency in the discharge of its responsibilities under the Act. There is no requirement that the information disclosed be relevant to a specific investigation or even to an area of investigation.

The U.S. Federal Court of Appeal (2nd Cir) decision in *ACLU v Clapper* (May 7, 2015) illustrates how broadly security agencies are prepared to interpret relevancy in order to pursue their mandates. The plaintiff-appellants challenged the NSA's use of Section 215 of the *Patriot Act* to collect and data mine metadata associated with the telephone calls of literally millions of American citizens as revealed by the Edward Snowden leaks. The NSA's program had been repeatedly authorized by secret orders made by the Foreign Intelligence Surveillance Court. The threshold test for obtaining the information was relevancy: could the information be subpoenaed into the court before a grand jury. The government noted that this test of relevancy casted a very broad net and that "`relevance' is an extremely generous standard." They cited cases where "courts have authorized discovery of large volumes of information" "to identify within that volume smaller amounts of information that could directly bear on the matter." The appellants challenged the government's use of Section 215 to conduct such surveillance on two bases: first, the statute required the information to be "relevant to an authorized investigation," not a general area of investigation such as terrorism; and second, section 251 violated the Fourth[10] and First[11]

[7] *Privacy Act* Section 7 (a) Use of personal information, Section 8(1) Disclosure of personal information
[8] Submission to the Standing Committee on Public Safety Security of the House of Commons, Office of the Privacy Commissioner of Canada, March 5, 2015
[9] *R. v. Grant*, 2015 SCC 9, [2015] 1 S.C.R. 475 at para. 18.
[10] IV Amendment: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
[11] I Amendment: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendments of the U.S. Constitution. Ultimately, the appellants prevailed on the first argument based on the court's interpretation of Section 215 to confine its scope to authorized investigations into specific matters rather than the general area of terrorism and counterterrorism. The court did not reach the constitutional issues.

There are no such statutory restraints on relevancy in Section 5(1) and any restrictions on its scope will have to come either from *Charter* litigation or political oversight based on internal reviews of the actual operation of the section.

The second striking feature of the *SCISA* is its expansive reframing of the government's role in national security matters. This comes from the new definition of an activity that undermines the security of Canada which encompasses far more activities than terrorism:

> "activity that undermines the security of Canada" means any activity, including any of the following activities, if it undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada:
>
> > (a) interference with the capability of the Government of Canada in relation to intelligence, defence, border operations, public safety, the administration of justice, diplomatic or consular relations, or the economic or financial stability of Canada;
> >
> > (b) changing or unduly influencing a government in Canada by force or unlawful means;
> >
> > (c) espionage, sabotage or covert foreign-influenced activities;
> >
> > (d) terrorism;
> >
> > (e) proliferation of nuclear, chemical, radiological or biological weapons;
> >
> > (f) interference with critical infrastructure;
> >
> > (g) interference with the global information infrastructure, as defined in section 273.61 of the National Defence Act;
> >
> > (h) an activity that causes serious harm to a person or their property because of that person's association with Canada; and
> >
> > (i) an activity that takes place in Canada and undermines the security of another state.
>
> For greater certainty, it does not include advocacy, protest, dissent and artistic expression.

The breadth of the shopping list in the definition is startling. Environmental demonstrators and First Nation activists opposed to pipeline projects risk coming under the "interference with critical infrastructure" or the "interference with … the economic or financial stability of Canada" subclauses. Québec sovereigntists and First Nation leaders may be said to be undermining the sovereignty or territorial integrity of Canada by pursuing their claims. International organizations opposed to climate change may be said to be "unduly influencing a government in Canada … by … unlawful means" by

funding or supporting domestic opposition to the Oil Sands. The RCMP and CSIS have in the past targeted these types of individuals and groups for surveillance and investigation. The *SCISA* now grants legitimacy to these acts.

During the debates on Bill C-51, the Harper government argued that the definition had internal limits on its scope: an activity coming within one of the itemized categories would only fall within the definition if the activity also "undermines the sovereignty, security or integrity of Canada or the lives or the security of the people of Canada." This interpretation generally conforms to the syntax employed in the definition but is hard to reconcile with the category, "an activity that takes place in Canada and undermines the security of another state,[12]" given that such an activity may have no bearing on the security of Canada. Reliance of the term "undermines" also offers little meaningful limitation. Undermining in this context connotes a secretive insidious process in which small seemingly innocuous or imperceptible actions may have long term deleterious effects.[13] The preamble to the Act supports this interpretation, ominously noting that "activities that undermine the security of Canada are often carried out in a clandestine, deceptive or hostile manner, are increasingly global, complex and sophisticated, and often emerge and evolve rapidly." Thus the Act gives support to a national security agenda of constant vigilance and surveillance of even seemingly benign or innocent activities that may, nevertheless, have the potential to undermine the security of Canada. Finally, given that the Act provides no review mechanism, it is difficult to see what administrative or legal processes exist that could restrain or restrict an unduly expansive interpretation of the authority conferred by the Act on the 17 designated security agencies. The interpretation of Section 215 of the *Patriot Act* by the NSA and the FIS Court provides a cautionary tale about the dangers of secrecy and lack of transparency in these matters.

One of the ironies surrounding the debate over Bill C-51 was that the Harper government promoted the *SCISA* as its response to the recommendations of the *Air India Inquiry* and to the *Arar Inquiry.* Nothing could be further from the truth. The *Air India Inquiry* centered in part of the failure of CSIS and the RCMP to share relevant information. CSIS and the RCMP have been well aware of this problem for at least the last fifteen years and have set protocols and procedures in place to address it with some apparent success. The *SCISA* does not offer further resources or solutions for this problem; instead the Act vastly compounds the problems of co-ordination by designating 17 agencies to collect and analyze information relevant to national security without providing any structure or coordinating mechanism. The *Arar Inquiry* centered in part on the dangers of information sharing: the RCMP shared misleading and inaccurate information about Mr. Arar to their U.S. counterparts who then acted on that information by kidnapping Mr. Arar and rendering him to Syria for torture and interrogation. Again the *SCISA*, if anything, by facilitating the sharing and disclosing of personal information without meaningful

[12] This category may have been intended to encompass international boycotts such as the Boycott, Divestment and Sanctions (BDS) movement against Israel.

[13] OED: Undermine:

3. *fig.* To work secretly or stealthily against (a person); to overthrow or supplant by underhand means.

7. a. To weaken, injure, destroy or ruin, surreptitiously or insidiously.
b. To weaken or destroy (the health or constitution) by degrees; to sap.

review and controls increases the risk of another Arar case occurring. The *SCISA* expressly provides that it does not restrict the further disclosure of information acquired[14] and insulates information disclosed from production or disclosure in a criminal or civil procedure.[15] Where the *SCISA* may be considered to respond to the *Air India Inquiry* and to the *Arar Inquiry* is in its provision for protection from civil proceedings against any person disclosing information under the Act in good faith.[16]

Bill C-51 also amended the *Income Tax Act* to provide easier access to tax returns by the 17 national security agencies designated by the *SCISA*. In general, the *Income Tax Act* has strict controls on the release of taxpayer information.[17] Bill C-51 loosened these controls to allow for release of taxpayer information if "there are reasonable grounds to suspect that the information would be relevant to" an investigation into whether an activity may constitute a threat to the security of Canada as defined by the *CSIS Act* or into whether a terrorism offence under the *Criminal Code* may have been committed.[18] A warrant is no longer required. As well, there is no restriction on an agency further disclosing taxpayer information to another agency, domestic or foreign, or to a third party.

This is a real issue as illustrated by the recent report that CSIS illegally accessed taxpayer information.[19] In August 2014, CSIS notified its review body, the Security Intelligence Review Committee (SIRC), of an incident where a CSIS officer had obtained taxpayer information from the Canada Revenue Agency (CRA) without a Federal Court warrant. Pre-Bill C-51, the *Income Tax Act* required CSIS to obtain a warrant to obtain such information. The Federal Court first raised the question about how CSIS had obtained taxpayer information used in a warrant application. In response, SIRC conducted a review at CSIS's request and found that this was not an isolated incident by a single officer contrary to how CSIS management portrayed the situation. In fact there were multiple instances of a particular CSIS office obtaining information from CRA absent a warrant. Subsequently CSIS advised that all of the CRA information obtained absent a warrant had been deleted from the operational database. In fact, most of the information remained within the database until SIRC brought this to CSIS's attention.

Bill C-51's solution is to obviate the need for a warrant in these situations, thereby opening the door to wide-ranging access to taxpayer information.

The extent to which *SCISA* could come under *Charter* scrutiny is unclear. The jurisprudence surrounding state access to and use and distribution of personal information is complex with many unresolved issues.

The Supreme Court of Canada has recognized that Section 8 of the *Charter* offers some measure of protection of a person's reasonable expectation of privacy in personal information held by a third party.

---

[14] Section 6 and 7(b) of the *SCISA*.
[15] Section 7(1) of the *SCISA*.
[16] Section 9 of the *SCISA*.
[17] See Section 241(1) of the *ITA.*
[18] Section 241(9) of the *ITA.*
[19] See SIRC Annual Report 2014–2015: Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review, September 30, 2015, SIRC's Inquiry into CSIS's Collection of Canada Revenue Agency Information Request by CSIS Director.

In *Spencer*[20] the police obtained access without a warrant to Internet subscriber information from the defendant's Internet Service Provider (ISP) in order to link him to the IP address used to download child pornography. The Court held that this constituted a search, that the defendant had a reasonable expectation of privacy in that information, and that neither the ISP nor the police could rely on the administrative access provisions in Section 7(3)(c.1)(ii) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to justify access to the information. Without the unconstitutionally obtained subscriber information, there were no reasonable grounds for the search warrant for the defendant's computer and the search therefore violated Section 8. Having granted that boon to the defendant, the Supreme Court then proceeded to take it away by admitting the evidence under Section 24(2).

Spencer is helpful in the *SCISA* context in two ways. First the Court took a broad view of the use that could be made of the information rather than relying on the narrow literal approach urged by the Crown to the effect that it was just bare subscriber data. The Court recognized that the IP address was a link to the defendant's entire history of online activity. Second the Court explicitly recognized that there is an informational component to the privacy interest protected by the *Charter*. Informational privacy in turn comprises three overlapping understandings: privacy as secrecy, privacy as control and privacy as anonymity. Privacy as control is particularly relevant to the *SCISA* context. The Court described the interests as follows:

> [40] Privacy also includes the related but wider notion of control over, access to and use of information, that is, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others": A. F. Westin, *Privacy and Freedom* (1970), at p. 7, cited in *Tessling*, at para. 23. La Forest J. made this point in *Dyment*. The understanding of informational privacy as control "derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit" (*Dyment*, at p. 429, quoting from *Privacy and Computers*, the Report of the Task Force established by the Department of Communications/Department of Justice (1972), at p. 13). Even though the information will be communicated and cannot be thought of as secret or confidential, "situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected" (pp. 429-30); see also *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 46.

Where *Spencer* falls down is in the convoluted and complex case specific analysis required to determine whether a person has a constitutionally protected reasonable expectation of privacy in a class of information. The factors to consider are many and various:

> [18] We assess whether there is a reasonable expectation of privacy in the totality of the circumstances by considering and weighing a large number of interrelated factors. These include both factors related to the nature of the privacy interests implicated by the state action and

[20] *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212.

> factors more directly concerned with the expectation of privacy, both subjectively and objectively viewed, in relation to those interests: see, e.g., *Tessling*, at para. 38; *Ward*, at para. 65. The fact that these considerations must be looked at in the "totality of the circumstances" underlines the point that they are often interrelated, that they must be adapted to the circumstances of the particular case and that they must be looked at as a whole.
>
> [19] The wide variety and number of factors that may be considered in assessing the reasonable expectation of privacy can be grouped under four main headings for analytical convenience: (1) the subject matter of the alleged search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances: *Tessling*, at para. 32; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at para. 27; *R. v. Cole*, 2012 SCC 53, [2012] 3 S.C.R. 34, at para. 40. However, this is not a purely factual inquiry. The reasonable expectation of privacy standard is normative rather than simply descriptive: *Tessling*, at para. 42. Thus, while the analysis is sensitive to the factual context, it is inevitably "laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy": *Patrick*, at para. 14; see also *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 34, and *Ward*, at paras. 81-85.

Not expectedly, results will vary when applying this type of multifactorial analysis to different situations with a reasonable expectation to privacy being recognized in some cases and not others.

This type of analysis is unsuited to regulating access to and use and distribution of the large number of personal information databases held by the Government of Canada. Uncertainty favours access since a case can always be made that there is no reasonable expectation of privacy in a particular data set or that expediency and necessity trumps the privacy interest. This analysis also does not address the effect of the aggregation of seemingly innocuous scattered bits of information in order to assemble a revealing picture of the person's work, residence, family, interests, activities, social contacts, financial and medical status, and other core biographical details.[21]

An alternative approach is to apply the Section 8 requirement that a search must be no more intrusive than is reasonably necessary to achieve its objectives[22] to limit the ambit of *SCISA* data mining. This principle was applied in *R. v. Rogers Communications.*[23] The police had obtained Production Orders to compel two telecommunication companies to provide cell tower dumps of all records of cellular traffic through cell towers near the scenes of a series of robberies. The Orders would have required production of the cell phone traffic records of over 40,000 subscribers. The Justice issued a declaration

[21] See for example Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (January 23, 2014) at pages 155 to 161 dealing with the revealing nature of the telephone metadata gathered by the NSA pursuant to Section 215 of the *Patriot Act*.
[22] *R v. Vu* [2013] 3 S.C.R. 657 at paras 21-2.
[23] 2016 ONSC 70, Sproat J.

that the Orders violated Section 8 because they went far beyond what was reasonably necessary to gather evidence concerning the commission of the crimes under investigation.[24] Again this approach requires that there be a search, that is, that the persons affected had a reasonable expectation of privacy in the information, and leads back into the *Spencer* type analysis.

The *SCISA* is singularly deficient in recordkeeping, oversight, review, and reporting mechanisms that may provide acceptable alternative accountability measures to a notice requirement. As a result, it may run afoul of the Section 8 requirement of accountability. In *Tse*[25] the Supreme Court of Canada found that Section 8 required accountability measures to allow for *ex post facto* review of police conduct. In that case, the Court struck down a wiretap provision that authorized a police officer to intercept private communications, without prior judicial authorization, on reasonable grounds that the interception is immediately necessary to prevent an unlawful act that would cause serious harm. The legislative scheme did not require that notice be given to persons whose private communications had thus been intercepted and accordingly did not provide any mechanism to permit oversight of the police use of this power. The Court adopted the submission by the Criminal Lawyers Association that:

> . . . notice is neither irrelevant to s. 8 protection, nor is it a "weak" way of protecting s. 8 rights, simply because it occurs *after* the invasion of privacy. A requirement of after-the-fact notice casts a constitutionally important light back on the statutorily authorised intrusion. The right to privacy implies not just freedom from unreasonable search and seizure, but also the ability to identify and challenge such invasions, and to seek a meaningful remedy. Notice would enhance all these interests. In the case of a secret warrantless wiretap, notice to intercepted person stands almost alone as an external safeguard.

The Court recognized that there may be other mechanisms other than a notice provision to ensure accountability, including reports to Parliament, recordkeeping requirements, and restrictions on the use of the information. Again this argument is predicated on the applicability of Section 8.

Finally, Section 8 also can reach to the use and distribution of personal information. In *Wakeling* the Supreme Court of Canada found that in at least for exceptional and invasive forms of search, such as wiretaps, Section 8 extended to disclosures by law enforcement and that a continuing expectation of privacy in such information persists even after it has been lawfully collected. Thus to comply with Section 8, the disclosure must be authorized by law, the law itself must be reasonable, and the disclosure must be carried out in a reasonable manner.[26] *Wakeling* was concerned with the disclosure of wiretap evidence to U.S. law enforcement in the context of a cross-border drug investigation and the *Criminal Code* provision governing such disclosures. The revelations and recommendations of the *Arar Inquiry* formed a back drop to all three judgements. Arguably Section 8 could apply to *SCISA* disclosures that involve highly personal information where no proper protections and assurances exist to prevent misuse of the information.

---

[24] *Rogers supra* at para. 42.
[25] *R. v. Tse*, [2012] 1 S.C.R. 531, 2012 SCC 16
[26] *Wakeling v. United States of America*, 2014 SCC 72, [2014] 3 S.C.R. 549at paras.32-41.

An alternative approach is to look to the law surrounding *O'Connor* applications which control defense access to information held by a third party. The *O'Connor* procedure applies regardless of whether there is an expectation of privacy in the information, thus avoiding the multifactorial analysis outlined in *Spencer*.[27] Also, in contrast with the "whole government" approach implicit in the *SCISA*, the *O'Connor* jurisprudence explicitly rejects the notion that the government is one indivisible whole at least in the context of the Crown's obligation to make disclosure. In *McNeil* the Court noted that:

> [22] … A question then arises as to whether the "Crown", for disclosure purposes, encompasses other state authorities. The notion that all state authorities amount to a single "Crown" entity for the purposes of disclosure and production must be quickly rejected. It finds no support in law and, given our multi-tiered system of governance and the realities of Canada's geography, is unworkable in practice.[28]

Finally the *O'Connor* procedure requires the party seeking the information to justify access by an initial showing of "likely relevance" that is tied to a specific issue at stake in the proceeding.[29] The purpose of this requirement is to discourage "fishing expeditions"[30] and to prevent "speculative, fanciful, disruptive, unmeritorious, obstructive and time-consuming" production requests.[31] Requiring a specific focus for an access request coupled with a prohibition of speculative reasons would curtail the wholesale data mining of personal information data banks currently authorized by the *SCISA*.

What this mish-mash of legal issues and approaches perhaps best illustrates is the need of robust review and oversight mechanisms for the *SCISA* coupled with recordkeeping and audit trails to track the access to and distribution of the shared information. Effective administrative solutions are needed more so than legal remedies. Unfortunately, the *SCISA* does not address these needs. Currently only the Auditor General and the Privacy Commissioner have any review function in this area and both have disclaimed the necessary capabilities and competency to perform this task. The review agencies for CSIS, CSE and RCMP lack the authority to conduct cross-departmental reviews. As a result, the *SCISA* remains a black hole of information sharing.

Secure Air Travel Act[32]

The *Secure Air Travel Act* provided a legislative framework for the "no fly" list being operated by Transport Canada under the Passenger Protect Program. The *SATA* broadened the grounds for inclusion to add traveling by air for the purpose of committing a terrorist act to the existing ground of being a danger to transportation security. It created a more elaborate and formal process for Ministerial review of a listing followed by a limited right of appeal to the Federal Court.

---

[27] *McNeil supra* at para. 11.
[28] *R. v. McNeil*, [2009] 1 SCR 66, 2009 SCC 3
[29] Defined as "a reasonable possibility that the information is logically probative to an issue at trial or the competence of a witness to testify": *R. v. O'Connor*, [1995] 4 S.C.R. 411 at para. 22; *World Bank v. Wallace*, 2016 SCC 15 at paras. 112, 124 -133.
[30] *McNeil* at para. 28 and 29 ; *World Bank v. Wallace supra* at paras. 115
[31] *World Bank* at para. 130.
[32] In force August 1, 2015: SI/2015-0064.

The true extent of the program remains unclear as officials continue to provide only ballpark figures for the number of people on the "no fly" list. What has been clear is the extent of the administrative mismanagement of the list. For example, toddlers and small children have been tagged as potential security risk despite the absence of any requirement for air carriers to screen anyone under the age of 18.[33] The government has promised to address the problems.

A more substantive legal issue with the *SATA* are its procedures for enabling a person to challenge being named on the list. The appeal procedures in the Act are modelled on the pre-*Charkaoui* procedures for judicial review of security certificates under the *Immigration and Refugee Protection Act*[34] and neither afford the listed person basic fairness or conform to the principles of fundamental justice. They permit the Minister to justify the decision in an *ex parte in camera* hearing before the judge if disclosure of the information would be injurious to national security or to the safety of any person Minister. But there is no provision for review by a Special Advocate of information presented *ex parte* and *in camera* by the Minister to the judge.

The Supreme Court of Canada struck down pre-*Charkaoui* procedure in the *IRPA* for secret hearings as being a violation of Section 7 of the *Charter* that was not saved by Section 1. The constitutionality of the *SATA* appeal procedure will turn in part on the assessment of the decision's impact on the life of the individual. The greater the effect on the individual, the greater is the need for procedural protections to meet the common law duty of fairness and the requirements of fundamental justice under Section 7 of the *Charter*.[35] The effect on the appellants in *Charkaoui* was patently dire - indefinite detention in Canada, the prospect of deportation to torture, detention and even death, and stigmatization as terrorist – and easily justified the full procedural protections of Section 7 of the *Charter*.

The effect of being put on the "no fly" list while not as dire are nevertheless very serious. The individual affected will likely not be able to return to his or her country of origin to visit family and friends. Travel to other countries will likely be next to impossible, given U.S. travel restrictions. Even air travel to other parts of Canada may be impossible if the airplane travels over any U.S. territory. The airline may simply refuse to allow the person to travel on the basis of transportation security. There is also the related stigmatization of being labelled a terrorist or threat to aviation safety. The listing will be shared with other countries and, in particular, the U.S.[36] and may have further serious repercussions for the person in those countries.

The more pertinent constitutional issue is whether the secret hearing process in the Act meets a minimal impairment standard. The question should not be so much an assessment of how serious the effect of the decision is on the life of the individual but whether a secret hearing is required when a reasonable workable alternative – a Special Advocate – is available.

---

[33] No-fly list flags more Canadian toddlers as security risks, cbc.ca January 4, 2016; Markham boy, 6, on no-fly list, parents say, cbc.ca January 3, 2016; *Secure Air Travel Regulations* SOR/2015-181, Section 5(1).

[34] *Charkaoui v. Canada (Citizenship and Immigration)*, [2007] 1 SCR 350, 2007 SCC 9 Appendix

[35] *Charkaoui supra* at para. 25 citing *Suresh v. Canada (Minister of Citizenship and Immigration)*, [2002] 1 S.C.R. 3, 2002 SCC 1 and *Dehghani v. Canada (Minister of Employment and Immigration)*, 1993 CanLII 128 (SCC), [1993] 1 S.C.R. 1053, at p. 1077, per Iacobucci J.

[36] Sections 11 and 12 of the *Secure Air Travel Act*.

The *SATA* has its own unique procedural deficiencies. Unlike the Passenger Protect Program where the interdicted person was informed why he or she could not board the aircraft, the *SATA* makes it an offence to give such notice.[37] Worse, the person has 60 days from the date of denial to apply to the Minister to review the decision to the Minister even though he or she may not know they are on the "no-fly" list, let alone the reason for it.

Finally there remains the more fundamental question whether an appeal modelled on a judicial review standard where the appellant must show that the decision was unreasonable is appropriate. A reasonable alternative would be to require the Minister to justify the listing.

Criminal Code Amendments[38]

Bill C-51 created a new terrorist propaganda offence[39] and lower the threshold for obtaining a terrorism peace bond to "reasonable grounds that another person may commit a terrorism offence." The Liberal government has intimated that it will amend the terrorist propaganda offence but not the terrorism peace bond provisions. To date, it does not appear that any charges have been laid under the terrorist propaganda section. Proceedings have been brought under the new terrorism peace bond section with one reported case, *Canada (Attorney General) v. Driver*.[40] Proceedings had been initiated against Driver before the new terrorism peace bond provisions came into force and were continued under the new provisions in accordance with the transitional provisions in Bill C-51.[41]

Bill C-51 creates a new offence of Advocating or promoting commission of terrorism offences:

> 83.221 (1) Every person who, by communicating statements, knowingly advocates or promotes the commission of terrorism offences in general—other than an offence under this section—while knowing that any of those offences will be committed or being reckless as to whether any of those offences may be committed, as a result of such communication, is guilty of an indictable offence and is liable to imprisonment for a term of not more than five years.

"Communicating statements" would include written or spoken words and "gestures, signs or other visible representations,"[42] and thus could conceivably include displaying a flag of proscribed terrorist groups such as Hamas.

The most notable deficiency in the new provision is the failure to provide for a defense of truth or good faith expression of an opinion on a religious subject or a matter of public interest. The hate speech provisions expressly provide for such a defense.[43] The majority of the Supreme Court of Canada in

---

[37] Sections 20 and 23 of the *Secure Air Travel Act*.
[38] The terrorist propaganda offence came into force on June 18, 2015; the terrorist peace bond section on July 18, 2015;: SI/2015-0064.
[39] Section 83.221, Advocating or Promoting Commission of Terrorism Offences
[40] *Canada (Attorney General) v. Driver*, 2016 MBPC 3 (Man. Prov. Ct., Rolston P.J.)
[41] Section 28, *Anti-Terrorism Act, 2015*.
[42] Section 83.221 (2) incorporating the definitions of "Communicating" and "Statements" in Section 319(7) which relate to the Public Incitement of Hatred offences.
[43] Section 319 (3): No person shall be convicted of an offence under subsection (2) [Wilful promotion of hatred]

Keegstra used the availability of these statutory defenses as part of its finding that the promoting hatred offence in Section 319(2) met the minimal impairment branch of the Section 1 analysis.[44] Conversely the absence of such a defense may be fatal to the constitutional validity of the new offense. It may be this omission the Liberal government is planning to correct when it promises to "narrow overly broad definitions, such as defining "terrorist propaganda" more clearly."[45]

The new offense has other problems. There are obvious overbreadth issues. The subject matter "the commission of terrorism offences in general" is vast and inchoate, particularly given how broadly drafted are the terrorism offences in the *Criminal Code* to begin with. The use of the term "in general" points towards an offence where advocating or promoting a specific activity is not necessary; a statement of support or an argument in favour of a proscribed terrorist group may suffice. The communication may be private and not intended for public dissemination.

The use of the term "knowingly" as opposed to "wilfully" will also make the new offence harder to justify under Section 1 of the *Charter*. The use of "wilfully" in the promotion of hatred offence was relied on by Martin JA in *Buzzanga and Durocher*[46] to import a requirement that a defendant intend the promotion of hatred and foresee that that consequence be substantially certain. Dickson C.J. for the majority in *Keegstra* relied heavily on this interpretation to find that the promoting hatred offence met the minimal impairment branch of the Section 1 analysis. "Knowingly" does not necessarily connote a higher requirement of purposefulness and could simply apply to the act of communicating rather than any intended consequences or purpose.

Finally the consequences of the advocacy or promotion of terrorism in general need not be substantially certain; rather the defendant need only be "reckless as to whether any of those offences may be committed." To translate this into the usual legal formula for what constitutes recklessness, it would suffice only that the defendant be aware that his or her conduct could bring about the result prohibited (that a terrorism offence may be committed) and persists despite the risk.[47] This would not require that there be an obvious and serious risk that a terrorism offence will be committed. There also may not be any specific circumstances against which to assess the risk. Typically recklessness under the *Criminal Code* is moored to specific consequences, such as being reckless whether a fire will cause damage to property,[48] or to the immediate circumstances in which the act is being committed, such as discharging a

---

(a) if he establishes that the statements communicated were true;
(b) if, in good faith, the person expressed or attempted to establish by an argument an opinion on a religious subject or an opinion based on a belief in a religious text;
(c) if the statements were relevant to any subject of public interest, the discussion of which was for the public benefit, and if on reasonable grounds he believed them to be true; or
(d) if, in good faith, he intended to point out, for the purpose of removal, matters producing or tending to produce feelings of hatred toward an identifiable group in Canada.

[44] *R. v. Keegstra*, [1990] 3 S.C.R. 697 at pages 778-783;
[45] Liberal Party of Canada, The Platform, Bill C-51, https://www.liberal.ca/realchange/bill-c-51/.
[46] (1979) 49 C.C.C. (2d) 369 (Ont. C.A.)
[47] *R. v. Sansregret* [1985] 1 SCR 570 at 581-2.
[48] Sections 433 and 434 of the *Criminal Code*; more generally see Section 429(1) for the extended definition of Wilfully causing event to occur.

firearm in a food court, thereby being reckless as to the lives and safety of other persons.[49] The free flow of information once communicated makes it impossible for a speaker to know who may receive the message and more importantly what meaning they will ascribe to it.

The principal change in the terrorist peace bond provisions, other than giving them their own section of the *Criminal Code,* was to lower the threshold for getting such a peace bond from "reasonable grounds that another person will commit a terrorism offence" to "reasonable grounds that another person may commit a terrorism offence."

The defendant in *Canada (Attorney General) v. Driver* argued that the change lowered the standard of proof to proof of a mere possibility that an individual will commit an offence and hence did not accord with the principles of fundamental justice. The trial judge agreed that the use of the word "may" meant that the Crown need only establish a "mere possibility" that the defendant would commit a terrorism offence. Despite this, he rejected the defense argument. The judge interpreted the section as requiring proof on a balance of probabilities that the defendant may commit a terrorism offence, thus maintaining the appearance of a constitutionally viable standard of proof but also creating the challenging concept of probably showing a possibility. The court found that the provision was not void for vagueness or overbroad, relying an interpretation that terrorism offences did not apply to "the expression of political, religious or ideological thoughts, beliefs or opinions."[50] Laudable as that interpretation may be, it is not entirely correct; the limitation cited by the judge only applies to the definition of "terrorist activities" and not to terrorism offences in general or in particular to the new offence of advocating or promoting terrorism offences.

Importantly, the court found that the condition that a defendant participate in a treatment program was overbroad because it could lead to court-ordered deprogramming of defendants who held unpopular ideological beliefs. Mr. Driver had originally been released on bail subject to various onerous conditions including one that he participate in "religious counseling."

The Crown conceded in *Driver* the obvious point that the terrorism peace bond provisions have the potential to deprive a defendant of his or her liberty. What is missing in the judgment is an assessment of the extent to which the provisions may deprive a defendant of liberty and security of person. The requirements of fundamental justice should be informed by the severity of the impact of the provisions on the defendant's interests in liberty and security of person.[51] The impact of the terrorism peace bond provisions can be very onerous. The defendant can be ordered into house arrest,[52] required to wear an electronic monitoring device,[53]sent into internal exile,[54] made to "participate in a treatment program,"[55]required to abstain from drugs or alcohol,[56] and ordered to surrender his or her passport.[57]

---

[49] Section 244.2(1).
[50] Section 83.01(1.1). The limitation only applies to the definition of "terrorist activity" which in turn forms part of the *actus reus* for some but not all terrorism offences.
[51] See for example *Charakaoui* (*supra*):
[52] Section 810.011(6)(c): "to return to and remain at their place of residence at specified times"
[53] Section 810.011(6)(b)
[54] Section 810.011(10): "remain within a specified geographic area"
[55] Section 810.011(6)(a)

As well, the judge can add "any reasonable conditions ... that the judge considers desirable,"[58] which can include non-communication and non-association clauses and bans and restrictions on the use of the Internet and social media and on the possession or use of computers, tablets or cellphones. The period can be up to 5 years for a defendant previously convicted of terrorism offence; up to 1 year otherwise. There is no restriction on multiple renewals.

Furthermore, the terrorism order has penal consequences. Refusing to agree to the conditions can result in up to 12 months in jail. A breach of a condition is punishable on indictment to up to 4 years in jail; on summary conviction up to 18 months.

Given the potential deprivation of liberty and security a defendant faces, the threshold to impose the deprivation should be correspondingly higher. Proving that probably there is a possibility that the defendant may commit a terrorist offense is too low a standard. This conforms with the sliding scale of standards in the criminal law context. For example, a brief detention may require only reasonable suspicion; a longer detention reasonable and probable grounds.[59] A Section 7 analysis avoids the more problematic analysis of whether the defendant can be said to come under Section 11 of the *Charter* as a "person charged with an offence." There is the analytic problem of determining whether the new provisions have crossed the line from preventive to punitive measure coupled with the courts general reluctance to dilute the protections for a person charged with an offence in Section 11.[60]

A related issue is whether the threshold of a reasonable possibility that the defendant may commit a terrorism offence is overbroad in the sense that it will inevitably generate false positives. In *Chelil*, the Supreme Court of Canada recognized that a reasonable suspicion standard (equivalent to a reasonable possibility) necessarily means that there is a reasonable possibility that the police will get it wrong.[61] This may be a reasonable price to pay where the detention is brief or the search not unduly intrusive. It should be unacceptable where a person's liberty for a year or more is at stake. The threshold issue is particularly important in the case of peace bonds where there is no easy way to determine if there is a false positive. The solution is to require at least a reasonable probable standard.

Canadian Security Intelligence Service Act Amendments[62]

The most controversial aspect of Bill C-51 is the granting of new powers to CSIS to take measures to disrupt perceived threats to the security of Canada and to apply to a Federal Court judge for a warrant authorizing CSIS to break the law and violate the *Charter* if necessary to take such measures.

---

[56] Section 810.011(6)(d)
[57] Section 810.011(9)
[58] Section 810.011(6)
[59] See for example *R. v. Mann*, [2004] 3 S.C.R. 59 (only reasonable suspicion required for an investigative detention which should be brief in duration);
[60] See for example *R. v. Budreo*, 142 CCC (3d) 225 (ON CA)
[61] *R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220 at para. 27 - 28; *R. v. McKenzie*, 2013 SCC 50, [2013] 3 S.C.R. 250 at para. 85;
[62] In force on the date of proclamation, June 18, 2015.

In March of this year, the Director of CSIS reported that the agency had resorted to disruption measures less than two dozen times, none of which required a warrant.[63] The Director did not provide any details of the measures taken. It is possible that at least some of the measure were taken outside of Canada. CSIS is only required to obtain a warrant only if the measures would contravene the *Charter* or be "contrary to other Canadian law."[64] It is unknown whether any of the measures taken contravened the law of any other country. An earlier bill, Bill C-44, gave CSIS explicit jurisdiction to perform its duties and functions "within or outside of Canada."[65] Bill C-51 explicitly extended this to permit disruption measures to be taken "within or outside of Canada" and, for greater certainty, provided that a warrant can authorize measures outside of Canada "[w]ithout regard to any other law, including that of any foreign state."[66]

The constitutionality of the warrant powers under Section 21.1 is very much a live issue. Section 12.1(3) explicitly gives a judge the power to authorize CSIS to take measures that violate the *Charter*:

> 12.1 (3) The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the Canadian Charter of Rights and Freedoms or will be contrary to other Canadian law, unless the Service is authorized to take them by a warrant issued under section 21.1.

Michael Duffy, Senior General Counsel, National Security Law, Department of Justice, justified the provision by a theory that the judge's authorization operates as a reasonable limit prescribed by law under Section 1 of the *Charter*. He explained it as follows to the House Standing Committee on Public Safety and National Security on March 31, 2015:

> The judge is being put in precisely the position of looking at the facts of a particular case and determining whether or not the rights that are at issue are reasonably restricted. That is precisely one of the functions that is allowed a judge under the charter. Section one provides for that determination, and that's what the bill in fact provides for.
>
> It is not correct, in our submission, that in fact the bill is in any way co-opting the court or anyone else into sanctioning a charter violation. It goes to a judge precisely for that reason, to make sure that the charter will not be violated. The charter violation occurs when a particular right is restricted in a way that is not reasonable, and that is the inquiry that a judge makes under the statute.

At first blush, this argument seems to confuse adjudicative functions with legislative functions. How can a judge's order be in itself a reasonable limit prescribed by law? Consider the Supreme Court of Canada decision in *Multani*[67]where the court considered the *Charter* implications of an administrative decision

[63] The Standing Senate Committee on National Security and Defence, March 7, 2016.
[64] Section 12.1(3) *Canadian Security Intelligence Service Act*.
[65] Section 12(2) *Canadian Security Intelligence Service Act*.
[66] Sections 12.1(1), 21.1(1) and 21.1(4).
[67] *Multani v. Commission scolaire Marguerite-Bourgeoys*, [2006] 1 SCR 256, 2006 SCC 6

by a school board to ban kirpans.[68] The school board acted pursuant to a very broad discretion conferred by the *Education Act* to approve rules of conduct and safety measures. The majority of the court found that the administrative order violated freedom of religion and was not justified as a reasonable limit under Section 1. Deschamps and Abella JJ. concurred in the result but held that only a legislative law qualified as a limit prescribed by law; an administrative decision could not.[69] The majority considered their argument but rejected it: an administrative order made pursuant to a valid enabling statute could operate as a limit prescribed by law.[70] Subsequently the Supreme Court of Canada in *Doré* backed away from the *Multani* approach of approaching such orders from a purely *Charter* perspective and returned to a more flexible administrative law approach that avoided the strictures of a full Section 1 analysis and the issue of what "prescribed by law" means.[71] However, the broad characterization of what "prescribed by law" by the majority in *Multani* still stands for the moment.

There are cogent reasons for not adopting the government's interpretation of the *Charter* as it applies to Sections 12.1(3) and 21.1 without the need to resort to complex legal analysis, appeals to Diceyan theories of parliamentary sovereignty, or philosophic considerations on what is a law. To begin with, virtually the only limit on a judge's discretion is the ambit of the CSIS application before him or her. There are no limits on subject matter or territorial application. This is in contrast to an administrative order which is constrained to a particular area and a specific jurisdiction. Second, the judge's order is made in secret, making challenging the decision impossible. Third, there is no provision for appeal or judicial review to test whether the judge's decision is a reasonable limit. In a sense, the judge's decision is self-justifying.

A second issue is whether these provisions accord with the *Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment*. One of main objections to the new disruption measures was that they could include arbitrary detention, illegal rendition or even torture. Given the revelations surrounding the CIA's "enhanced" interrogation programs and "black sites" and MI6's illegal renditions to Libya, among others, the concerns are real. Section 12.2 limits the measures power as follows:

> Prohibited conduct
>
> 12.2 (1) In taking measures to reduce a threat to the security of Canada, the Service shall not
>
> (a) cause, intentionally or by criminal negligence, death or bodily harm to an individual;
>
> (b) wilfully attempt in any manner to obstruct, pervert or defeat the course of justice; or
>
> (c) violate the sexual integrity of an individual.

[68] *Multani v. Commission scolaire Marguerite-Bourgeoys*, [2006] 1 SCR 256, 2006 SCC 6
[69] See paras. 100 to 125;
[70] See paras. 21 to 23;
[71] *Doré v. Barreau du Québec*, [2012] 1 SCR 395, 2012 SCC 12. The decision of the court was written by Abella J.

Omitted are prohibitions against detention, rendition or torture. Amendments to include these prohibitions were opposed by the Harper government and defeated. The question is whether this failure to act violates the positive duty on signatories like Canada to "take effective legislative, administrative, judicial or other measures to prevent acts of torture in any territory under its jurisdiction."[72]

The breadth and secrecy of the disruptive measures provisions point strongly to the need for more robust review.

Immigration and Refugee Protection Act (IRPA) Amendments[73]

The amendments to the *IRPA* contained in Bill C-51 are the latest salvo by the government in the long war over the Security Certificate system. The amendments are intended to make it easier for the Minister to refuse to disclose sensitive information to the Special Advocate appointed to protect the interests of a person challenging a Security Certificate. Bill C-44 provided companion amendments to create a form of informer privilege for human sources, who, after having received a promise of confidentiality from CSIS, has provided information to the CSIS.

The current battle for access to the information relevant to the issuance of a Security Certificate begins with *Charkaoui I* where the Supreme Court of Canada struck down the Security Certificate regime in place then. That regime provided for an *ex parte in camera* hearing in which the Minister could present to a Federal Court judge information the disclosure of which "would be injurious to national security or to the safety of any person." The person named and his or her counsel were excluded from this private hearing. The Supreme Court of Canada recognized the manifest unfairness of this system, found it denied the person named fundamental justice, and struck it down as not justified under Section 1. In doing so, the court noted that a Special Advocate system modeled on the UK practice may satisfy the minimal impairment requirement in the Section 1 analysis.

The government accordingly amended the *IRPA* to provide for access by a Special Advocate to the secret information relied by the Minister in the *ex parte in camera* hearing before the judge. Subsequently the Supreme Court of Canada in *Harkat* upheld the constitutional validity of the new provisions.[74]

Following the amendments, the Supreme Court of Canada in *Charkaoui II* clarified the Minister's disclosure obligations in Security Certificate hearings.[75] Mr. Charkaoui sought a stay of proceedings relating to the Security Certificate issued against him on the basis that the government breached its duty to disclose relevant information in its possession to him. The Supreme Court held that CSIS had a duty to disclose all information in its possession regarding the person named in a security certificate. This included a duty to retain relevant information. This information must be put before the judge hearing the case. In turn, the judge must then disclose the information to the person named in the security certificate, except to the extent that disclosure might, in the judge's view, endanger Canada's security.

[72] Article 2 1. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.
[73] In force July 1, 2015: SI/2015-0064.
[74] *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37, [2014] 2 S.C.R. 33
[75] *Charkaoui v. Canada (Citizenship and Immigration)*, [2008] 2 S.C.R. 326, 2008 SCC 38

These developments had two unpleasant consequences for the Minister: first, the Special Advocates could point out the deficiencies and inaccuracies in the hitherto unscrutinized information. Second, the Minister may have to grant disclosure of information that it did not want to disclose even to a Special Advocate.

The *Almrei* case illustrates the first consequence of full disclosure and access by a Special Advocate. Hassan Almrei had come to Canada in 1999 and claimed refugee status. On October 19, 2001, he was detained on a Security Certificate and his case was referred for review by the Federal Court. The Federal Court heard evidence from the Minister in a hearing from which Almrei was excluded and upheld the certificate. Mr. Almrei launched a series of court challenges to this decision and ultimately succeeded as one of the appellants in *Charkaoui*. On February 22, 2008, the day the post-*Charkaoui* amendments to the *IRPA* came into effect the Minister issued a new Security Certificate against him. By that point Mr. Almrei had been in custody for over 7 years. A new hearing was held, this time with a Special Advocate having access to the secret information relied on by the Minister and to the further disclosure of CSIS files relevant to Mr. Almrei's case pursuant to *Charkaoui II*. The further disclosure requested by the Special Advocates revealed surveillance and intercept reports that contradicted human source reports on which CSIS and the Ministers relied. The court found in the circumstances that the respondent had breached the duty of candor. In the result the Certificate was quashed.

The *Charkaoui* case illustrates the second consequence. Rather than comply with its disclosure obligations, the Minister chose not to proceed with the Security Certificate against him, saying that disclosing such information would endanger national security. As a result, in 2009 the Certificate was declared null and void.

Bill C-51 attempts to change this landscape by allowing the judge to exempt the Minister from its disclosure obligations on the basis that the exempted information does not enable the person named to be reasonably informed of the case against him or her.[76] The constitutionality of this provision will be in issue, given that it permits the Minister to withhold information regarding the person named in the Certificate and arguably enables the withholding of relevant information. It also provides for a system of interlocutory appeals by the Minister against an unfavourable disclosure decision, thereby raising the prospect of lengthy delays while the person named languishes in custody pending the disposition of the interlocutory appeals.[77]

Thus in a sense we have come full circle from the robust disclosure regime of the *Security of Canada Information Sharing Act* where the designated security agencies have virtually unfettered access to personal information to the new Security Certificate regime where the security agencies increasingly seek to restrict or deny a person named in a Certificate access to relevant information in the name of national security.

[76] Sections 83(1)(c.1) and (c.2) of the *Immigration and Refugee Protection Act*.
[77] Sections 86.1, 87 and 87.1 of the *Immigration and Refugee Protection Act*.