Curing Complexity: Moving Forward from the Toronto 18 on Intelligence-to-Evidence

JAY PELLETIER AND CRAIG FORCESE [*]

ABSTRACT

This chapter addresses one aspect of Canada's "intelligence to evidence" (I2E) problem that both featured in the Toronto 18 prosecutions and has since occupied courts (and presumably agencies): criminal trial challenges to warrants supported by intelligence and used to collect information employed either to seed a subsequent RCMP investigation (or wiretap warrant) or as evidence of guilt in a subsequent prosecution. These matters implicate so-called *Garofoli* applications. The awkward interface between these *Garofoli* applications and I2E may constitute the single most perplexing (and possibly resolvable) I2E issue. Specifically, this chapter asks whether *Garofoli* applications heard *ex parte* (that is, with only the government party before the court) and *in camera* (that is, in a closed court) would be constitutionally viable under section 7 of the *Charter*. We conclude that closed material *Garofoli* applications with built-in procedural protections — namely statutorily-mandated special advocates — would meet constitutional standards.

---

[*] This chapter represents the views of the authors and not of the organizations with which they may be affiliated. At the time it was written in 2019, Craig Forcese was Jay Pelletier's professor, as Mr Pelletier completed his JD degree at the University of Ottawa. Mr. Pelletier is now counsel with the Department of Justice. Craig Forcese is a professor of law at the University of Ottawa. The views expressed in this article are those of the authors and do not reflect those of the Department of Justice, the Government of Canada, or any institution with which they are affiliated.

I. INTRODUCTION

The Toronto 18 trials were successful prosecutions. They were also complex, even as measured against the complexity of almost all Canadian post-*Charter* criminal proceedings. Complexity stemmed from the novelty of the matter — terrorism offences were uncommon and raised questions of interpretation. But the organization of Canada's anti-terrorism bureaucracy also contributed to their complexity. As Murray and Huzulak (Chapter 8) and Michaelson (Chapter 6) discuss, two separate but equal agencies lead investigations into terrorism matters in Canada: the police, and especially the Royal Canadian Mounted Police (RCMP), empowered to investigate and charge for terrorism crimes; and the Canadian Security Intelligence Service (CSIS), responsible for gathering intelligence on threats to the security of Canada, including prospective terrorists.

These two agencies cooperate, but only from consciously-created siloes and in a choreographed manner. Sometimes this choreography means agencies do not share seemingly important information — and, especially, CSIS does not share with the police. Consider this passage from *Ahmad*:

> CSIS was aware of the location of the terrorist training camp ... This information was not provided to the RCMP, who had to uncover that information by their own means. Sometimes CSIS was aware that the RCMP were following the wrong person, or that they had surveillance on a house when the target of the surveillance was not inside, but [CSIS] did not intervene.[1]

In describing these events, the court did not condemn CSIS. Instead, it explained how Canada has managed inter-agency relationships: parallel RCMP and CSIS investigations. The court described a "firewall" between "parallel" investigations run by CSIS and the RCMP, one that tries to avoid CSIS intelligence "contaminating the police investigation". Observers have sometimes called this system "less is more"[2] – the less information shared to meet inter-agency needs, the better. At present, CSIS and the RCMP call the bureaucratic framework designed to manage this segregated

---

1 R v. Ahmad, 2009 CanLII 84776 at para 43 (ON SC) [*Ahmad*, 2009]. For a more recent example in which CSIS did not share information with police in a terrorism case, see at R v. Peshdary, 2017 ONSC 1225 at para 20.

2 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Final Report*, vol. 2 (Ottawa: Public Works and Government Services Canada, 2010), 543.

investigative system One Vision (now in its second version as "One Vision 2.0").[3]

One Vision 2.0 attempts to regulate an institutional distance produced by history, institutional culture, and different legal mandates. But it also responds, however imperfectly, to legal preoccupations that have assumed quasi-mythical status in Canada's security and intelligence community. The "intelligence-to-evidence" (I2E) dilemma is the short-hand for describing these concerns. Today, more than a decade after the Toronto 18, intelligence-to-evidence remains a challenge. David Vigneault, the Director of CSIS, described the I2E process as one of Canada's most significant national security challenges.[4] Bob Paulson, former Commissioner of the RCMP, expressed concern that the I2E process could compromise public safety.[5] With the rise of the extremist traveller phenomenon, the I2E problem has become even more acute, as Canada has struggled to prosecute extremist travellers for crimes committed while abroad.

This chapter does not address the full scope of I2E issues. In their chapter, Murray and Huzulak note how I2E drives CSIS and the RCMP's siloed relationship, reducing the sharing of actionable intelligence and potentially jeopardizing public safety. One of us, meanwhile, has written a paper discussing these same issues and proposing several solutions.[6] Here, we focus on a specific I2E problem, one that both featured in the Toronto 18 prosecutions and has since occupied courts (and presumably agencies): criminal trial challenges to warrants supported by intelligence and used to collect information employed either to seed a subsequent RCMP investigation (or wiretap warrant) or as evidence of guilt in a subsequent prosecution. These matters implicate so-called *Garofoli* applications. The awkward interface between these *Garofoli* applications and I2E may constitute the single most perplexing (and possibly resolvable) I2E issue.

---

3 "CSIS-RCMP Framework for Cooperation One Vision 2.0," Secret Law Gazette, last modified November 10, 2015, http://secretlaw.omeka.net/items/show/21.

4 David Vigneault, "An INTREPID Podsight: CSIS Director David Vigneault," episode 36, in *INTREPID*, podcast, https://www.intrepidpodcast.com/podcast/.

5 Robert Paulson, "An INTREPID Podsight with Rob Paulson (Former Commissioner of the RCMP)," episode 41, in *INTREPID*, podcast, https://www.intrepidpodcast.com/pocast/.

6 Craig Forcese, "Threading the Needle: Structural Reform & Canada's Intelligence-to-Evidence Dilemma," *Manitoba Law Journal* 42, no. 4 (2019): 131. Portions of this chapter incorporate discussions drawn from this article, setting the stage for a more detailed analysis of the *Garofoli* process.

Specifically, this chapter asks whether *Garofoli* applications heard *ex parte* (that is, with only the government party before the court) and *in camera* (that is, in a closed court) would be constitutionally viable under section 7 of the *Charter*. For ease of reference, we call these *ex parte* and *in camera* proceedings "closed material proceedings." We conclude closed material *Garofoli* applications with built-in procedural protections — namely statutorily-mandated special advocates — would meet constitutional standards.

We organize our following discussion into two parts. First, we offer an overview of disclosure rules in Canadian criminal law as they relate to intelligence. Second, we focus on how *Garofoli* applications might be organized to avoid unnecessary I2E dilemmas that prejudice legitimate state interests while doing nothing to enhance trial fairness.

II. Disclosure Rules and Evidentiary Intelligence

A. Overview of I2E Evidentiary-Intelligence Shield Issues

"Intelligence-to-evidence" is the unwieldy phrase used to describe several discrete types of issues. The first — at issue in the *Ahmad* matter — is the movement of intelligence procured by intelligence services to support law enforcement, typically the police. We call that the "actionable-intelligence" issue.

Police or other law enforcement agencies could act on actionable-intelligence without worrying about its use as evidence, perhaps to pre-empt a public safety threat. However, law enforcement agencies exist to investigate crimes, and securing convictions for offenders depends on legal proceedings. To perform their mission, police cannot disregard the laws of evidence, at least not without running the risk of a court then invalidating their conduct. Likewise, intelligence agencies must contemplate how police in their more legalized environment will use — and especially, disclose — the information intelligence services provide. For these reasons, actionable-intelligence is tied to a second, closely related component of I2E: something we call the "evidentiary-intelligence" issue. Evidentiary-intelligence has two aspects: the "evidentiary-intelligence sword" and the "evidentiary-intelligence shield."

The evidentiary-intelligence sword issue involves the use of intelligence in legal proceedings to justify state action. For example, the prosecutor may wish to use intelligence provided by CSIS to the RCMP to prove that an

accused has committed a terrorist offence. At issue here is the use of intelligence as evidence in a legal proceeding, either to justify police conduct or to prevail in a legal dispute. In using intelligence as a sword, police and prosecutors must worry about the quality of the information, measured against evidentiary standards. In comparison, the evidentiary-intelligence shield is about CSIS and its lawyers protecting intelligence from disclosure as part of a legal proceeding. For example, the government often seeks to protect CSIS intelligence about the accused from disclosure to the defence. CSIS wishes to ensure that its "Crown jewels"[7] — its targets, means, methods, and sources — are not disclosed to an accused who may, in fact, be a threat actor and in open court.[8]

Evidentiary-intelligence shield issues are most acute in criminal proceedings, where Canada's exceptionally broad disclosure obligations put CSIS's intelligence — and the sensitive sources and investigative methods used to collect it — at risk of being exposed in open court. In *R v. Stinchcombe*, the Supreme Court of Canada held that section 7 of the *Charter* requires the Crown to disclose all relevant material to the accused to ensure the accused can make full answer and defence. "Relevance" was defined as anything which is clearly not irrelevant to an issue at trial.[9]

The Crown, for the purposes of *Stinchcombe* disclosure, constitutes the Crown attorneys prosecuting the offence and the police investigating the offence, including their investigative file and any police "third-party" material that is "obviously relevant to the accused's case."[10] This "third party" is any entity other than the Crown and the police. Any third-party information already in police or Crown possession is presumptively subject to *Stinchcombe*.[11] However, CSIS — a third party — is not subject to *Stinchcombe* unless its information is already in the Crown's possession or

---

7 Canada, *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182: Final Report*, in *Air India Flight 182: A Canadian Tragedy*, vol, 3 (Ottawa: Supply and Services, 2010), 195.

8 The standard, CSIS "boilerplate" description of information CSIS will protect is set out in Huang v. Canada (Attorney-General), 2017 FC 662 at para 23, aff'd 2018 FCA 109.

9 R v. Stinchcombe, [1991] 3 S.C.R. 326 at 338–39, 1991 CanLII 45; Morris v. The Queen, [1983] 2 S.C.R. 190 at 200–01, 1 D.L.R. (4th) 385; R v. McNeil, 2009 SCC 3 at paras 17–18.

10 *McNeil*, SCC at paras 22–25, 59.

11 *McNeil*, SCC at paras 22–25, 59.

the CSIS investigation becomes so interwoven with the police investigation that there is only one investigation leading to prosecution.[12]

As a third-party, CSIS (or any other intelligence service) does not escape disclosure obligations. The legal regime for third-party disclosure in criminal trials is found in *R v. O'Connor*. Under *O'Connor*, the accused must demonstrate that the information sought is "likely relevant." This threshold is different than *Stinchcombe*, requiring the defence to demonstrate that there is a "reasonable possibility" that the information is logically probative to an issue at trial.[13] If the defence meets this threshold, the judge must examine the information to weigh the salutary benefits and deleterious effects of production, and then determine whether non-production constitutes a reasonable limit on the accused's right to make full answer and defence. The Court will examine several factors when applying the balancing test.[14]

Since the *O'Connor* regime provides more (procedural) protection, CSIS goes to great lengths to remain a third party. However, *O'Connor*'s protections should not be exaggerated because the likely relevance threshold is not a high bar and the balancing test does not, at all, weigh in CSIS's favour. Thus, even as a third party, CSIS is at great risk of having its sources and methods dragged into criminal proceedings.

It is noteworthy, however, that both *Stinchcombe* and *O'Connor* are subject to privileges and immunities. As such, CSIS may invoke a special national security-related public interest immunity under section 38 of the *Canada Evidence Act* to protect information, the disclosure of which would be injurious to international affairs, national defence, or national security.

B. Evidentiary Intelligence and the Warrant Process

1. Police Warrants

I2E disclosure issues may arise where evidence in a prosecution comes from a wiretap (or possibly, other forms of a search warrant). Judges issue police wiretaps after a closed-door (*in camera*) proceeding in which only the

---

12 *Ahmad* 2009, CanLII at para 12.

13 R v. O'Connor, [1995] 4 S.C.R. 411 at paras 19–22, 130 D.L.R. (4th) 235.

14 *O'Connor*, S.C.R. at paras 30–32. These factors include: the extent to which the information necessary for the accused's ability to make full answer and defence; the probative value of the information; the degree of reasonable expectation of privacy in the information; whether the disclosure is premised on discriminatory belief; and potential prejudice to the third-party's dignity, privacy, and security.

government side appears (*ex parte*) — in other words, a closed material proceeding. Police applications in these closed material proceedings must be supported by evidence, compiled through an "Information to Obtain" (ITO). ITOs include an affidavit in which police affiants spell out the facts for their "reasonable grounds to believe" (also known as "reasonable and probable grounds") that interception of specified people's communications may assist in the investigation of an offence.[15]

A wiretap is constitutional if it meets the strict requirements in the *Criminal Code*.[16] A defendant prosecuted because of evidence stemming from the wiretap may wish to challenge the admissibility of that evidence by showing that a court unlawfully issued the warrant or the police used the warrant in an unlawful manner. Defendants mount this challenge through a *Garofoli* application.[17] The material issues in a *Garofoli* application are, only, whether the record before the original, warrant-authorizing judge satisfied the statutory preconditions for the warrant and whether that record accurately reflected what the affiant knew or ought to have known. If the record fails this standard, the question then is whether the errors were egregious enough to affect the issuance of the warrant. The reviewing judge is not to substitute their view in place of the issuing judge's; a *Garofoli* application is not a *de novo* review. But in making their assessments, reviewing judges will excise any extraneous or improperly obtained information from the ITO and amplify the record with any relevant, correct evidence that was available at the time of the warrant.[18] The reviewing judge will invalidate the warrant where, upon review of the material before the authorizing judge, as amplified, the reviewing judge believes there was "no basis upon which the authorizing judge could be satisfied that the preconditions for the granting of the authorization existed."[19]

To make these *Garofoli* applications, defendants need all the information about the original warrant proceedings — and this requires disclosure to the defence. For a police warrant, the information

---

15 Criminal Code, R.S.C. 1985, c. C-46, s. 185(1). Sometimes called "reasonable and probable grounds" in the constitutional caselaw, "reasonable grounds to believe" is much lower than the criminal trial standard of "beyond a reasonable doubt." Instead, it is defined as a "credibly-based probability" or "reasonable probability." See R v. Debot, [1989] 2 S.C.R. 1140, 37 OAC 1.

16 See discussion on this point in *Huang*, FC at para 14.

17 R v. Garofoli, [1990] 2 S.C.R. 1421, 43 OAC 1.

18 *Garofoli*, S.C.R. at 1452.

19 R v. Pires; R v. Lising, 2005 SCC 66 at para 7.

undergirding a warrant may already be part of the police investigative file, already disclosable to the defence under *Stinchcombe*'s broad relevance test. Here, the *Garofoli* challenge does not broaden the aperture of disclosure already applicable to the actual criminal trial. However, if the Crown and police have not disclosed the supporting information related to the warrant (because it is clearly irrelevant to the trial under *Stinchcombe*), this supporting information is now potentially disclosable under this new *Garofoli* challenge. In a *Garofoli* challenge, the affidavit supporting the warrant authorization and the documents before the authorizing judge are presumptively disclosable.[20] The defence may also cross-examine the affiant with leave of the court. The court will grant leave where cross-examination is necessary to make full answer and defence. To this end, the defence must show cross-examination will elicit testimony tending to discredit the existence of one of the pre-conditions to the warrant authorization.[21]

Still, the threshold for disclosure — relevance — does not authorize a fishing expedition through documents never before the affiant whose affidavit supported the warrant application, in part because the courts have been sensitive about revealing confidential sources.[22] To access these materials, the accused must, "establish some basis for believing that there is a reasonable possibility that disclosure will be of assistance on the application" to challenge the warrant.[23] Applying this standard, lower courts have found instances where some police information — for example, notes kept by the handler of a confidential informant — are irrelevant, both for the trial and for challenging a search warrant.[24]

2. Police Warrants Supported by CSIS Information

CSIS can collect intelligence through wiretaps authorized by the Federal Court under its own separate *CSIS Act* warrant procedures. Here, CSIS supports the warrant application with an affidavit asserting the facts believed, on reasonable grounds, to show why the warrant would enable CSIS to investigate a threat to the security of Canada.[25]

---

20 World Bank Group v. Wallace, 2016 SCC 15 at para 134.

21 *Garofoli*, S.C.R. at 1465.

22 *World Bank Group*, SCC at para 129 *et seq*.

23 R v. Ahmed et al., 2012 ONSC 4893 at paras 30–31, an approach cited without objection in *World Bank Group*, SCC at para 131.

24 See e.g., R v. Ali, 2013 ONSC 2629, cited without objection in *World Bank Group*, SCC at para 131.

25 Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23, s. 21 [CSIS Act].

In investigating under a warrant, CSIS sometimes discovers actionable-intelligence. In a functioning I2E system, CSIS will share this actionable-intelligence with the RCMP in an advisory letter – that is, a letter from CSIS to the RCMP containing intelligence and permitting its use in legal proceedings.[26] The CSIS information would then find its way into the police investigation, one that may culminate in charges and a prosecution. Consequently, CSIS may worry that the contents of its wiretap intercept (or potentially, other types of searches), shared to further an RCMP investigation, might later attract *Garofoli*-style scrutiny of CSIS's own, original Federal Court authorization and the basis for it.[27] That original CSIS warrant authorization may have been supported by confidential, human source information, foreign origin intelligence, and signals intelligence, all of which CSIS would not wish to disclosed in open court. Moreover, the CSIS warrant may be broad, focused on targets beyond the person(s) charged. This information is extraneous to the criminal proceeding, and CSIS will need to protect it from disclosure.

The Toronto 18 case demonstrates the complexity of this specific I2E dilemma. There, the defence initiated *Garofoli* applications on five *Criminal Code* RCMP wiretaps, the first of which relied on three CSIS advisory letters to establish reasonable and probable grounds.[28] The defence alleged CSIS's failure to disclose information in its advisory letters was misleading and that the destruction of CSIS operational notes violated section 7 of the *Charter*.[29]

The court held that CSIS's destruction of the notes violated section 7 of the *Charter* and that CSIS, though it did not act misleadingly, breached its duty of candour to the court. As a result, the court excised any information relating to the destroyed notes and any information that was presented inconsistently with the duty of candour. Moreover, the Crown prosecutors opted not to rely on any information obtained through CSIS warrants or information derived from CSIS warrants to avoid lengthy and

---

26 An "advisory letter" "contains information that may be used by the RCMP to obtain search warrants, authorizations for electronic surveillance, or otherwise used in court. In the case of Advisory letters, CSIS requires the opportunity to review any applications for judicial authorizations prior to filing." See Secret Law Gazette, "CSIS-RCMP Framework," 2.

27 For an example, see Peshdary v. Canada (Attorney General), 2018 FC 850; Peshdary v. Canada (Attorney General), 2018 FC 911.

28 R v. Ahmad, 2009 CanLII 84784 (ON SC) at paras 3, 17-18 [*Ahmad 84784*].

29 *Ahmad 84784*, CanLII at para 29.

complex *Garofoli* applications at the Federal Court.[30] As a result, the Crown relied on virtually no CSIS information at the *Garofoli* application. The only information relied on with a nexus to CSIS was that which the human source had collected during his time with CSIS and then gave to the RCMP after the hand-off of that source to the police. The court found, nevertheless, that the warrant was properly authorized.[31]

As this decision suggests, CSIS's warranted intercept activity must stand up to scrutiny where the information collected under it becomes evidentiary-intelligence used in a police investigation. The CSIS warrant under which CSIS collected this intelligence — and its supporting information — becomes material, triggering disclosure obligations. But to add to the complexity, CSIS is likely a "third party," not the Crown. And where CSIS has the resulting *O'Connor* third-party status, disclosure of information relevant to this warrant-challenge purpose will follow the *O'Connor* two-step process: first, the defence will need to show the "likely relevance" of the documents being sought; second, if they do so, the documents are reviewed *in camera* and *ex parte* by the judge.[32] In practice, application of this test has meant that (at least redacted) copies of the CSIS affidavit supporting the CSIS warrant will be disclosed, along with any supporting material actually before the warrant-authorizing judge.[33] Courts may also oblige disclosure of draft warrant applications.[34] There is also the possibility that the CSIS affiant may be cross-examined, but only with leave of the court and confined to the question of whether the affiant knew or

---

30 *Ahmad 84784*, CanLII at paras 76–78, 83–86, 133–38. The court found that CSIS's advisory letters did not comply with the duty of full, frank, and fair disclosure. The letters filtered out unreliable information pertaining to material matters, but the letters did not disclose that it excluded information. The court expressed concern that the letters could trick the reader. However, it found that CSIS did not intend to mislead by excluding such information.

31 *Ahmad 84784*, CanLII at paras 34–36, 182–83, 212, 215–36.

32 R v. Jaser, 2014 ONSC 6052. See also Canada (Attorney-General) v. Huang, 2018 FCA 109 at para 19.

33 *Jaser*, ONSC at para 18 (observing that the "CSIS Affidavit on which the Federal Court authorization depends easily meets the first stage O'Connor/McNeil test of 'likely relevance'"); R v. Alizadeh, 2013 ONSC 5417. The test is whether the documents will be of probative value on the issues in the application – that is, the validity of the warrant. More specifically: "would the justice have had reason to be concerned about issuing the warrant had he or she been made aware of the other facts." See R v. Peshdary, 2018 ONSC 2487 at para 9 *et seq*.

34 R v. Peshdary, 2018 ONSC 1358.

ought to have known about errors or omissions in the warrant application.[35] It is unlikely that source materials undergirding the warrant documents must also be disclosed. Where CSIS is a third party under the *O'Connor* rule, lower courts have required the defence to show that "there is a factual basis for believing that the material sought will produce evidence tending to discredit a material pre-condition in the *CSIS Act* authorization."[36]

The full CSIS investigative file is not, in other words, thrown open to the public. But the interposition of a protracted and complex adjudication creates uncertainty and risk about how much sensitive CSIS sources, methods, and intelligence might end up in the public domain. Delay and complexity are compounded where CSIS concludes its intelligence at risk in a *Garofoli* application must be protected through a section 38 *Canada Evidence Act* proceeding.[37] Cumulatively, these evidentiary-intelligence shield uncertainties compound the I2E issue and add grit, thereby deterring the flow of actionable-intelligence from CSIS to the police. To summarize representative concerns:

- Sensitive CSIS information may be subject to disclosure in a *Garofoli* application on the relevance threshold, and CSIS will then need to decide whether to protect this information using the section 38 *Canada Evidence Act* national security privilege.
- If CSIS succeeds in protecting this information, it is no longer available to justify the issuance of the *CSIS Act* warrant. Should the remaining information not suffice to sustain the reasonableness of the warrant, the warrant will fail, as might a prosecution dependent on it or any RCMP warrant built on the information collected under the CSIS warrant.
- The collapse of the prosecution may follow, even though the CSIS warrant was perfectly lawful on the full record.

---

35 *Pires*; *Lising*, SCC at para 40 *et seq*. See also *World Bank Group*, SCC at para 121 *et seq*.

36 R v. Peshdary, 2018 ONSC 1358 at para 20. See also Peshdary v. Canada (Attorney General), 2018 FC 850.

37 For a fuller discussion of trials and tribulations associated with section 38 *Canada Evidence Act* proceedings, see Craig Forcese and Kent Roach, *False Security: The Radicalization of Canadian Anti-terrorism* (Toronto: Irwin Law, 2015), 305 *et seq*; Forcese, "Threading the Needle".

This scenario is a happy outcome for the accused, but no broader public interest is served by it. It introduces a structural impediment to the use of the criminal law in national security matters where the criminal law is the most appropriate state tool. Again, it is worth recalling that in their *Garofoli* application, the Crown opted not to rely on CSIS information to avoid disclosure entanglements. It will not always be the case, though, that other information is available to use as evidence in a criminal case.

The question is, therefore, whether there is a way to reconcile the defendant's fair trial interests with the legitimate interests of CSIS in protecting its properly sensitive materials, in a manner that avoids this game of "disclosure chicken."

III. Closing *Garofoli* Applications

A. Overview

We believe that a warrant issued via a closed material proceeding can be reviewed in a closed material proceeding, when scrutinized to ensure that the statutory niceties required for its issuance were met. Put another way, there is no principled reason to demand that a warrant, which may be constitutionally issued in a closed material, one-sided process, must then be reviewed in a fully open proceeding. A rule permitting an intelligence warrant to be reviewed in a closed material proceeding would create no more risk to sensitive CSIS sources, means, and methods than did the original CSIS warrant application. In this manner, it would eliminate the problem of disclosure chicken, at least in this area.

The public safety advantages are obvious. A statutory scheme allowing for *Garofoli* applications to be heard in a closed material hearing would streamline, and potentially facilitate, more seamless CSIS and police investigations by creating a zone in which CSIS could share intelligence with the RCMP without worrying about disclosure at all. Doing so would ensure that CSIS information, other than that which is (already) relevant under *Stinchcombe* or *O'Connor*, is protected from external disclosure while still helping the RCMP build a criminal case.[38]

Under this proposal, CSIS could share intelligence derived from sensitive sources that it otherwise would not share with the RCMP, such as

---

[38] *World Bank Group*, SCC at paras 129–32. See *Ahmad 84784*, CanLII for an example of how the Crown was unwilling to disclose sensitive information at a *Garofoli* application and, as a consequence, could not rely on the information.

human sources, signals intelligence (SIGINT), or foreign-origin information given in confidence. For example, CSIS may rely on Communications Security Establishment or foreign-origin SIGINT to collect intelligence because such agencies have the technical capability to target extremist travellers abroad. However, the government would never allow SIGINT to be exposed in court, as it is often derived from extremely sensitive technical means that would be rendered useless if exposed. Under our proposal, this information could be used to support the police warrant, both in its initial issuance and subsequently in the closed *Garofoli* challenge. Likewise, CSIS could comfortably share intelligence that does form evidence on the merits where that evidence is derived from its own *CSIS Act* wiretaps, much like in *R v. Huang*.[39]

In this manner, CSIS intelligence could be used as an evidentiary-intelligence sword in defending CSIS (or dependent police) warrants or where wiretap information is used in trial. However, the intelligence, means, methods, and sources that are relevant in a *Garofoli* application are assessed behind closed doors, in an *ex parte* proceeding. That is, they remain shielded from external disclosure (but not from review *per se*). Closing *Garofoli* applications would also sidestep the impetus for collateral section 38 *Canada Evidence Act* proceedings in which intelligence agencies seek to protect their sensitive information from open court disclosure.[40] The key question is, however, whether a closed *Garofoli* application would be constitutional.[41]

B. The Constitutionality of Closed *Garofoli* Applications

Closing *Garofoli* applications appears inconsistent with the "open court principle" that "applies to all judicial proceedings," described as a "hallmark of a democratic society"[42] and protected by section 2 of the *Charter*. The principle is necessary for society to hold the courts accountable in administering justice fairly and impartially, thereby enhancing public

---

39 *Huang*, FCA.

40 This is not small improvement. Right now, *Garofoli* applications are collateral proceedings to criminal trials that then prompt their own collateral proceedings under section 38. It is hard to imagine a more byzantine system.

41 On this issue, see also Canada, *The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence,* by Kent Roach, in *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 Research Studies*, vol. 4, Catalogue No. Cp32-89/5-2010E (Ottawa: Supply and Services, 2010), 113.

42 Vancouver Sun (Re), 2004 SCC 43 at para 23.

confidence in the justice system.[43] Still, the open court principle is not absolute — indeed, it does not apply to the initial issuance of a warrant.[44] Nor does it preclude closed material proceedings in *Canada Evidence Act*, section 38 matters — cases in which the Federal Court's decision on disclosure may have a sizable impact on the defendant's ability to offer answer and defence.[45] The open court principle is, therefore, an unlikely barrier to a closed material *Garofoli* proceeding.

We focus, therefore, on a more serious objection: section 7 of the *Charter*, guaranteeing everyone "the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."[46]

1. The Right to a Make Full Answer and Defence

The right to make full answer and defence, though not a free-standing right, is a principle of fundamental justice under section 7's liberty interest.[47] *Stinchcombe*, described above, is the post-*Charter* starting point. Following *Stinchcombe*, the Supreme Court in *Dersch* and *Garofoli* was clear that withholding the contents of the sealed packet supporting the warrant — the affidavit — would violate the accused's right to make full answer and defence. It would effectively trap the accused in catch-22.[48]

However, in addition to establishing the Crown's disclosure obligations, *Stinchcombe* also established that the right to a fair trial does not mean a perfect trial. It held that where information is withheld, the trial judge must determine whether non-disclosure constitutes a "reasonable limit" on the right to full answer and defence.[49]

The Court has since held that section 7's principles of fundamental justice represent a spectrum of interests, from the rights of the accused to

---

43 *Vancouver Sun*, SCC at paras 23–26.

44 For the balancing exercise often used in relation to the "open court principle," see, e.g., Toronto Star Newspapers Ltd v. Ontario, 2005 SCC 41. In relation to sealing orders and warrants, see, e.g., R v. Nur, 2015 ONSC 7777; R v. Paugh, 2018 BCPC 149 (in relation to warrants).

45 See, e.g., Canada (Attorney General) v. Khawaja, 2007 FC 463.

46 Canadian Charter of Rights and Freedoms, s. 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11.

47 Dersch v. Canada (Attorney General), [1990] 2 S.C.R. 1505, 77 D.L.R. (4th) 473.

48 *Dersch*, S.C.R. at 1514–515.

49 *Stinchcombe*, S.C.R. at 340. The SCC also stated, in relation to summary conviction offences, that the content of the right to full answer and defence may be of a more limited nature.

broader societal concerns. Section 7 must be interpreted considering those interests and against the applicable principles and policies that have animated legislative and judicial practice in the field.[50] Courts must balance the interests of the individual and those of the state in providing "a fair and workable system of justice."[51] Accordingly, a fair trial is not the most advantageous or perfect trial from the accused's perspective. Rather, it is one "which satisfies the public interest in getting at the truth, while preserving basic procedural fairness to the accused."[52] The right to full answer and defence will be implicated where the information "is part of the case to meet or where the potential probative value is high."[53]

In the *Garofoli* context, the Supreme Court has recognized that while the accused is entitled to the packet underlying the warrant, the trial court may need to edit the contents of the packet to protect police sources and methods. In doing so, courts must balance competing public interests of police sources and investigative techniques with the right to make a full answer and defence, allowing maximum disclosure without rendering warrants useless as a law enforcement tool.[54] When weighing public interests, trial judges should consider the relevancy of the source's identity, prejudice to the sources or police methods, and whether there is an ongoing investigation.[55] In cases where the trial judge edits the contents, they may rely on the information if they provide a summary of the information to the accused such that the accused can still challenge the information.[56] Taken together, these authorities suggest there is no absolute right to disclosure in a *Garofoli* context to meet fair trial standards.

2. The Public Interest in Closed Material Garofoli Applications

The Supreme Court's jurisprudence suggests that the right to a fair trial requires a balancing between society's interest in a workable justice system

---

50 R v. Seaboyer, [1991] 2 S.C.R, 577 at 603, 83 D.L.R. (4th) 193; *O'Connor*, S.C.R. at paras 62, 65; R v. Harrer, [1995] 3 S.C.R. 562 at para 14, 128 D.L.R. (4th) 98. *O'Connor* and *Harrer* later affirmed that trial fairness requires balancing societal and individual interests.

51 *Harrer*, S.C.R. at para 14.

52 *Harrer*, S.C.R. at para 45 per McLachlin J, noting also a fair trial is a trial that appears fair from the perspectives both of the accused and the community.

53 R v. Mills, [1999] 3 S.C.R. 668 at paras 60, 71, 75, 94, 180 D.L.R. (4th) 1.

54 *Garofoli*, S.C.R. at 1458.

55 *Garofoli*, S.C.R. at 1460.

56 *Garofoli*, S.C.R. at 1461.

and individual interests. If the right to full answer and defence is not absolute, what qualities of intelligence gathering might justify a departure from the "perfect" trial? First, it is true that society's interest in ensuring accused persons can respond to the allegations is fundamental, especially because terrorism offences carry large penalties and stigma. However, society's interest in effectively prosecuting terrorism offences is also enormous.[57] Therefore, society's interest in ensuring the justice system can address, efficiently, I2E dilemmas is high.

Second, disclosure of CSIS information is even more likely to compromise security intelligence sources and methods than is the case when police disclose their own information in *Garofoli* challenges. Relative to police investigations, the confidentiality interest in security intelligence is often enduring because the collection of information is the end in and of itself, whereas the collection of information in law enforcement is a means to an end (that is, prosecution). As such, the disclosure of security intelligence in an affidavit is more likely to compromise ongoing investigations.[58] The result is the game of "disclosure chicken" which, as we have suggested, imperils public safety by encouraging security service silos. This reality engages important public interests.

Third, as bears repeating, the initial warrant at issue in a *Garofoli* process was issued in a closed material proceeding. There is one obvious reason for this: the presence of the warrant target would defeat the purpose of a covert communications interception warrant. This concern no longer matters once a target is arrested. That distinction, however, does not negate the public interests that remain engaged, even after arrest: disclosure of, for example, sensitive CSIS sources, means, and methods in a *Garofoli* proceeding could defeat other public interests, including the sustainability of other, ongoing investigations. At the same time, the impact of a closed *Garofoli* application on the accused's rights to full answer and defence would be indirect, at best. *Garofoli* applications do not test the merits of the criminal case. Rather, the issue is only whether there was a reasonable basis upon which the authorizing judge could find that the statutory preconditions for a warrant existed. Relevance under *Stinchcombe* or *O'Connor* in the application is tied to this narrow *Garofoli* test. The accused's right to know the criminal case to be met does not drive the

---

57 On these points, see R v. Hersi, 2019 ONCA 94 at para 54.

58 Henrie v. Canada (Security Intelligence Review Committee), [1989] 2 FC 229 at paras 11–12, 1988 CanLII 5686.

disclosure equation in this area.[59] Closed material *Garofoli* applications would have a narrow adverse effect on that core section 7 rights. Instead, *Garofoli* applications amount, more plausibly, to a proxy protection for section 8 *Charter* rights.[60] The most important virtue of a *Garofoli* challenge is to introduce a retrospective adversarial challenge to the original closed material proceeding.

3. The Defence and Public Interest in Adversarial Testing

Examined from this optic, an open *Garofoli* application imperils key public interests, chiefly (and indeed, arguably exclusively) to permit an accused and their counsel to introduce adversarialism to a prior closed material proceeding. If so, the obvious question is whether this goal of adversarial testing of the warrant might be accomplished through a means that does not produce the "disclosure chicken" problem and its resulting I2E dilemmas. We believe there are obvious lessons to be drawn from the special advocate system under the *Immigration and Refugee Protection Act* (*IRPA*) – lessons that apply even though the *IRPA* system is (technically) an administrative proceeding.

Under the *IRPA*, the Minister may issue a security certificate to detain and deport individuals (that is, the "named person") who the Minister has reasonable grounds to believe are inadmissible on security grounds.[61] A judge will then review the certificate for reasonableness, and the Minister may request that the review occur *ex parte* and *in camera*, excluding the named person or their counsel entirely. The named person may receive a summary of the information only if disclosure would not be injurious.[62] In the closed material proceeding, special advocates represent the named person's interests, subject to strictures on their ability to communicate with the defendant once they have seen the classified information.[63] Special advocates are security-cleared lawyers selected from an established roster of such advocates by the named person. These lawyers are then statutorily charged with representing the interests of the named person in the closed material proceedings. They have an unlimited ability to meet with the named person before reviewing the classified information. Thereafter, any

---

59 *Pires*; *Lising*, SCC at para 30; *Mills*, S.C.R. at paras 71, 75, 94.

60 See, *Garofoli*, S.C.R. at 1445 (addressing the rationale for *Garofoli* hearings with a focus on section 8 of the *Charter*).

61 Immigration and Refugee Protection Act, S.C. 2001, c. 27, ss. 77, 81 [IRPA].

62 IRPA, ss. 78–79.

63 IRPA, ss. 85–85.6.

further communication with the named person is done with permission of the judge. As this discussion suggests, special advocates are not in a solicitor-client relationship with named persons – such that they do not owe them the duty of candour that would otherwise exist and which would be difficult to reconcile with a system in which the special advocate must withhold classified information.

The immediate reaction of readers may be to bristle at the idea of applying this (controversial) model, developed in an *IRPA* context, to a (collateral) proceeding in a criminal trial. Our purpose is not to normalize a controversial immigration tool. Rather, we are interested in the jurisprudence developed under it and what it says about the ingredients of a section 7-compliant closed material proceedings. On this point, we observe the Supreme Court has been unambiguous in concluding section 7 applies to immigration security certificates. Security certificates are, in other words, about the same procedural rights to fundamental justice in play in *Garofoli* applications. Moreover, section 7 has been applied here to a system whose outcome, the Supreme Court has also acknowledged,[64] may be more serious than any penalty available under the criminal law. Specifically, the named person risks possible removal to torture or worse. The Supreme Court has also considered section 7 in relation to closed material proceedings that deal with the actual merits of the case – that is, matters where the right to know the case against the named person is squarely in play. Recall, this is not the case with *Garofoli* matters. Despite all these features of the security certificate regime that make its circumstances more pressing to trial fairness than *Garofoli* matters, the Court has upheld the constitutionality of closed material proceedings, when accompanied by special advocates.

If closed material proceedings are constitutional in this context, it is difficult to see how they would be unconstitutional in *Garofoli* challenges – collateral proceedings having much less immediate impacts on the defendant. To conclude otherwise would simply be formalistic, treating something associated with criminal proceedings as entitled (by simple categorization) to more constitutional protections than something with even graver impacts, done as part of administrative proceedings. We do not believe that the *Charter* operates according to such pigeonholes.

---

64 IRPA, ss. 85–85.6; Charkaoui v. Canada (Citizenship and Immigration), 2007 SCC 9 at paras 13–15 [*Charkaoui* 2007]; Canada (Citizenship and Immigration) v. Harkat, 2014 SCC 37 at para 1.

We turn, therefore, to lessons to be drawn from the jurisprudence on security certificates in designing closed material proceedings triggering section 7 interests.

C. Lessons from the Security Certificate Regime

The Supreme Court has considered the security certificate regime on two occasions. In *Charkaoui*, the Court found that the *IRPA* violated section 7 because it did not allow the named person to know and respond to the case against them.[65] In *Harkat*, the Court revisited the issue after Parliament established a system of special advocates and found that the regime complied with the *Charter*.[66]

In *Charkaoui*, the SCC affirmed that section 7 requires a fair process considering the interests at stake, the nature of the proceedings, and the context within which they take place. The procedures may reflect the exigencies of the security context as well as the need to protect sources and investigative methods. However, national security cannot justify a fundamentally unfair process.[67] Ultimately, the amount of disclosure must be proportionate to the individual's interests at stake. Circumstances (such as those in security certificates) that are closer to criminal proceedings will require greater disclosure.[68]

To meet section 7's requirements, the security certificate regime must afford the individual three procedural protections: the right to a hearing before an independent and impartial magistrate; a decision on the facts and law; and a proceeding that allows the individual to know and answer the case against them.[69] With respect to judicial independence, the Court found that the designated judge's role permitted sufficient challenge to the government's position to prevent state excess while assessing reasonableness.[70] As long as the judge did not allow the matter to morph into an inquisitorial proceeding with the judge seeking to advance either the Minister's or the defence's case, the judge's role would remain independent.[71]

---

65 *Charkaoui*, SCC 2007 at para 3.
66 *Harkat*, SCC at para 10.
67 *Charkaoui*, SCC 2007 at paras 23–25, 27, 58–61.
68 *Charkaoui*, SCC 2007 at paras 24–25.
69 *Charkaoui*, SCC 2007 at paras 29–31.
70 *Charkaoui*, SCC 2007 at paras 37, 39–42.
71 *Charkaoui*, SCC 2007 at paras 44–45.

Next, the Court held that the *IRPA* scheme, at that time, did not allow for decisions to be based on the facts and law, nor did it allow the named person to know and respond to the case against them. In security certificate proceedings, almost all information before the judge will be the government's information. The named person might not see any of the information because the procedure required the judge to withhold any information that would be injurious to security if it was disclosed. In turn, the Court found named persons might have insufficient disclosure to correct inaccuracies or challenge the credibility of the Minister's information.[72] Without sufficient defence submissions, the judge was at risk of deciding the matter without all facts. Therefore, the *IRPA* did not meet section 7's requirements for a fair hearing.[73]

The Court then found that the *IRPA* regime was not justified under section 1 of the *Charter*. The Court recognized that the non-disclosure of sensitive sources and methods is a sufficiently important objective.[74] However, the Supreme Court found that the *IRPA* was not minimally impairing on the fair hearing entitlement. Among other things, the Court stated that the United Kingdom's special advocate system might be a constitutionally acceptable procedure because it allows security-cleared lawyers to act on the named person's behalf in closed proceedings.[75]

Another possibility, noted by the Court, is to security-clear the named person's own lawyer. Security clearance is, however, a protracted and expensive process – and it cannot be assumed that every lawyer a named person might wish to employ would wish to subject themselves to this process. Nor, once the security-cleared defence lawyer is privy to classified information, might the lawyer wish to subject themselves to the permanent strictures of the *Security of Information Act*, with its stiff criminal sanctions for unauthorized disclosures.[76] Finally, the security-cleared defence lawyer would be in a conflict between their obligations under that *Act* and their obligations of disclosure to their client. As noted, this system would sit uncomfortably with the professional responsibility of a lawyer to be "honest

---

72 *Charkaoui*, SCC 2007 at paras 49-50, 53–55, 63–65.

73 *Charkaoui*, SCC 2007 at paras 63–65.

74 *Charkaoui*, SCC 2007 at paras 68–69 (disclosure could adversely affect Canada's ability to collect intelligence and receive intelligence from other countries).

75 *Charkaoui*, SCC 2007 at paras 80–82, 85–87.

76 R.S.C. 1985, c. O-5, ss. 13–14.

and candid" when advising clients.[77] The rules of professional conduct do allow information to be received "for counsel's eyes only," with client consent. But in regular litigation, these "protective orders" are rare – not least because "the entire solicitor–client relationship can break down if the client is unable to give instructions to counsel because they lack the relevant information."[78]

As noted, in responding to *Charkaoui*, Parliament did not opt for a security-cleared defence counsel model. Instead, it enacted the slightly different "special advocate" system. The Court considered the constitutionality of this proxy system of adversarialism in *Harkat*. There, it affirmed that, to meet section 7's requirements, the closed material procedure must use a "substantial substitute" to full disclosure, recognizing that the process must be flexible to accommodate national security concerns.[79] As such, the named person must, at minimum, know the "essence of the information… supporting the allegations" so that they can instruct the special advocates on how best to act on their behalf.[80] Moreover, the Supreme Court of Canada found the *IRPA* maintains the judge's role as gatekeeper of the fair proceeding because judges may only withhold information where there is a serious risk that disclosure would, in the judge's opinion, be injurious.[81]

Lastly, in assessing the special advocate regime, the Supreme Court recognized that the regime's restriction on the special advocate communicating with the named person once the former has seen the classified information is significant, but it does not render the regime unconstitutional. First, the restriction is not absolute: the judge has broad discretion to authorize communication and should apply that discretion liberally.[82] Second, the named person can freely send one-way communications to the special advocates, so the public summaries should help elicit information and instructions to the special advocate.[83] The

---

77 See, e.g., Ontario, *Rules of Professional Conduct*, Toronto: Law Society of Ontario, 2000, Rule 3.2-2.

78 William Horton, "Confidentiality in Canadian Litigation," in *Privilege and Confidentiality: An International Handbook, eds.* David Greenwald and Marc Russenberger *(London: Bloomsbury Professional, 2012)*, 68–69.

79 *Harkat*, SCC at paras 43, 46–47.

80 *Harkat*, SCC at paras 56–57.

81 *Harkat*, SCC at paras 61–63.

82 *Harkat*, SCC at paras 69–70.

83 *Harkat*, SCC at para 71.

Court concluded, therefore, that the *IRPA* regime is constitutional. However, the designated judge, as the gatekeeper, must always assess the overall fairness of the proceeding on a case-by-case basis.[84]

These decisions establish signposts for a closed material *Garofoli* proceeding. First, both proceedings implicate section 7's liberty interest.[85] The Supreme Court recognized that security certificates could have greater consequences than criminal proceedings.[86] *Garofoli* applications, in contrast, implicate the accused's liberty interest, but to a lesser extent than non-disclosure at trial because *Garofoli* applications do not adjudicate the merits of the case.[87] As we have suggested, security certificates, therefore, likely implicate section 7 interests to a greater extent than do *Garofoli* applications.[88]

Second, like with security certificates, closed material *Garofoli* applications are required to address a specific and pressing national security problem: I2E. Thus, the national security context should weigh in favour of closed material *Garofoli* applications.

Third, closed material *Garofoli* applications meet the basic criteria for a fair hearing, as outlined in *Charkaoui*.[89] Both the issuing and reviewing authorities for a warrant are judges, clothed in full judicial independence. The *Garofoli* reviewing court may vet CSIS or the RCMP's information and, indeed, has latitude to excise any problematic information and amplify information available at the time of the warrant. CSIS and the RCMP also have a duty of candour in closed material proceedings, requiring that applicants include both inculpatory, exculpatory, and any improperly obtained information in the warrant application and the *Garofoli* proceeding.[90]

Still, as with security certificate judges, the *Garofoli* judge can only assess that which the government puts before the court. Even with the duty of candour, the court would be hard-pressed to uncover information that supports excision and amplification. Rather, the defence must raise information that supports excision or amplification through their own

---

84 *Harkat*, SCC at para 77.

85 Charkaoui v. Canada (Citizenship and Immigration), 2008 SCC 38 at para 54; *Charkaoui*, SCC 2007 at paras 13–15; *Garofoli*, S.C.R. at 1461.

86 *Charkaoui*, SCC 2007 at para 13–15; *Harkat*, SCC at para 1.

87 *Pires; Lising*, SCC at para 30.

88 *Charkaoui*, SCC 2007 at paras 24–25.

89 *Charkaoui*, SCC 2007 at paras 29–31.

90 *Harkat*, SCC at paras 100–02; R v. Morelli, 2010 SCC 8 at para 102.

investigatory efforts or cross-examination. This is the virtue of adversarialism. Thus, just as with the security certificate regime, closed material *Garofoli* applications require a substantial substitute for disclosure to be constitutional.[91]

As found in *Harkat*, security-cleared special advocates are a substantial substitute because they can make oral submissions on the accused's behalf and cross-examine affiants in closed material proceedings.[92] However, special advocates can only be effective if the accused has minimum disclosure upon which they can adequately instruct the special advocate on how to challenge the Crown's case. Therefore, any statutory scheme for closed material *Garofoli* applications must afford the accused a summary of the information in the affidavit and must allow the special advocate to communicate with the accused, with leave of the court.[93]

The statutory scheme must also maintain the judge's role as the gatekeeper of fairness.[94] We propose two additional safeguards. The procedure should allow the trial judge to weigh the fair trial interest in disclosure against the public interest in non-disclosure – a procedure that the security certificate regime does not accommodate.[95] Further, in *Garofoli* applications, the defence must acquire leave of the court to cross-examine an affiant.[96] However, closed material *Garofoli* applications should follow the model of security certificates and endow special advocates with a right to cross-examine the affiant.[97]

IV. CONCLUSION

By all accounts, the Toronto 18 investigation and prosecutions were a success. However, they struggled with operational issues stemming from I2E dilemmas. CSIS failed to share intelligence with the RCMP, and at the

---

91 *Harkat*, SCC at paras 49–50, 53–55, 63–65.

92 *Harkat*, SCC at para 77.

93 *Harkat*, SCC at paras 56–57, 70.

94 *Harkat*, SCC at paras 61–63.

95 *Charkaoui*, SCC at para 77. The Court contrasted section 38 of the *Canada Evidence Act*'s balancing process with the lack thereof in the *IRPA* in its discussion of minimal impairment.

96 *Garofoli*, S.C.R. at 1465 (the defence must demonstrate a reasonable basis that cross-examination will elicit testimony tending to discredit the existence of one of the pre-conditions to the authorization).

97 IRPA, s. 85.2.

Garofoli application, the Crown was unable or unwilling to rely on CSIS information to justify the RCMP's ITO.

The I2E problem arises from the Crown's disclosure obligations under *Stinchcombe* and third-party disclosure obligations under *O'Connor*. The use of CSIS intelligence, and especially CSIS-warranted intercepts, raises pressing I2E challenges because of *Garofoli* applications. To improve (but not resolve) I2E in Canada, we propose a statutory scheme allowing *Garofoli* applications implicating information supplied by Canada's intelligence services to be heard as closed material proceedings, using special advocates representing the accused's interests. From a public safety perspective, closed material *Garofoli* applications would minimize the risk of public disclosure of (properly) sensitive information used to support CSIS warrants, which then produce information shared with the RCMP.

Critics of this view may immediately question the constitutionality of a closed material *Garofoli* proceeding. We believe that, properly legislated,[98] it would be constitutional. The reason for a *Garofoli* proceeding is to allow an accused to test – through an adversarial process – a warrant originally issued in a closed material warrant proceeding. That adversarial testing requires someone to press the state and take positions on the evidence that was before the issuing judge, adverse to the state's view. But that person need not be the accused or the accused's lawyer, who cannot (after all) bring new evidence unavailable at the time of the warrant and who, in a *Garofoli* challenge, is not confronting the criminal case to be met. Instead, a special advocate may play the adversarial role, just as they play an adversarial role in security certificate cases where the stakes are (in fact) higher than in *Garofoli* proceedings. In sum, closing *Garofoli* applications would help minimize the risk of Canadian national security trials becoming games of "disclosure chicken," in which technical application of Canada's complicated disclosure rules take primacy over the administration of justice while encouraging public safety-impairing siloes among Canada's security services.

---

98 We do not believe it advisable to establish this system based on some *ad hoc* inherent power of the court. First, it is not clear to us that the court has this power. Second, a statute is the best vessel through which to create the special advocate system and, indeed, that system already exists under *IRPA* and could be re-tasked for this new purpose. Third, *ad hoc* arrangements might wary between courts and jurisdictions, producing uncertainty and confusion.