



**SUPREME COURT OF CANADA**

**CITATION:** Canada (Citizenship and Immigration) v. Harkat, 2014 SCC 37      **DATE:** 20140514  
**DOCKET:** 34884

**BETWEEN:**

**Minister of Citizenship and Immigration and  
Minister of Public Safety and Emergency Preparedness**

Appellants/Respondents on cross-appeal  
and

**Mohamed Harkat**

Respondent/Appellant on cross-appeal

- and -

**Attorney General of Ontario, British Columbia Civil Liberties Association,  
Canadian Council of Criminal Defence Lawyers, Canadian Civil Liberties  
Association, Canadian Bar Association, Canadian Association of Refugee  
Lawyers, Canadian Council for Refugees, International Civil Liberties  
Monitoring Group, Canadian Council on American-Islamic Relations (now  
known as National Council of Canadian Muslims), Amnesty International and  
Criminal Lawyers' Association (Ontario)**

Interveners

**CORAM:** McLachlin C.J. and LeBel, Abella, Rothstein, Cromwell, Moldaver,  
Karakatsanis and Wagner JJ.

**REASONS FOR JUDGMENT:** McLachlin C.J. (LeBel, Rothstein, Moldaver, Karakatsanis  
(paras. 1 to 112) and Wagner JJ. concurring)

**JOINT REASONS DISSENTING IN** Abella and Cromwell JJ.

**PART ON THE APPEAL:**  
(paras. 113 to 139)

**NOTE:** This document is subject to editorial revision before its reproduction in final form in the *Canada Supreme Court Reports*.

---

CANADA (CITIZENSHIP AND IMMIGRATION) v. HARKAT

**Minister of Citizenship and  
Immigration and Minister of Public  
Safety and Emergency Preparedness**      *Appellants/Respondents on cross-appeal*

v.

**Mohamed Harkat**      *Respondent/Appellant on cross-appeal*

and

**Attorney General of Ontario,  
British Columbia Civil Liberties Association,  
Canadian Council of Criminal Defence Lawyers,  
Canadian Civil Liberties Association,  
Canadian Bar Association,  
Canadian Association of Refugee Lawyers,  
Canadian Council for Refugees,  
International Civil Liberties Monitoring Group,  
Canadian Council on American-Islamic Relations  
(now known as National Council of Canadian Muslims),  
Amnesty International and  
Criminal Lawyers' Association (Ontario)**      *Interveners*

**Indexed as: Canada (Citizenship and Immigration) v. Harkat**

**2014 SCC 37**

File No.: 34884.

2013: October 10, 11; 2014: May 14.

Present: McLachlin C.J. and LeBel, Abella, Rothstein, Cromwell, Moldaver, Karakatsanis and Wagner JJ.

ON APPEAL FROM THE FEDERAL COURT OF APPEAL

*Constitutional law — Charter of Rights — Right to life, liberty and security of person — Certificate issued against foreign national stating that he is inadmissible to Canada on national security grounds for allegedly engaging in terrorism — Named person challenging constitutionality of security certificate scheme on grounds that it prevents full disclosure and personal participation in hearings — Whether scheme under which security certificate issued deprives named person of right to life, liberty and security of person in accordance with principles of fundamental justice — Canadian Charter of Rights and Freedoms, s. 7 — Immigration and Refugee Protection Act, S.C. 2001, c. 27, ss. 77(2), 83(1)(c), 83(1)(d), 83(1)(e), 83(1)(h), 83(1)(i), 85.4(2), 85.5(b).*

*Immigration — Inadmissibility and removal — National security — Certificate issued against foreign national stating that he is inadmissible to Canada on national security grounds for allegedly engaging in terrorism — Judge reviewing reasonableness of certificate finding sufficient evidence to demonstrate that certificate was reasonable and upholding certificate — Whether designated judge erred in concluding that certificate was reasonable.*

*Evidence — Privilege — Informer privilege — Information used against named person obtained by CSIS from human sources — Whether CSIS human sources are covered by class privilege — Whether CSIS human sources can be cross-examined.*

*Constitutional law — Charter of Rights — Procedural fairness — Duty to disclose — Remedy — Summaries of intercepted conversations tendered as evidence against named person — Source materials for summaries destroyed in accordance with internal policy of CSIS — Whether destruction of source materials breached named person's right to procedural fairness — Whether designated judge erred in refusing to exclude summaries of intercepted conversations — Canadian Charter of Rights and Freedoms, ss. 7, 24(1).*

*Stay of proceedings — Duties of candour and utmost good faith — Fairness of process — Ex parte proceedings — Review of reasonableness of security certificate — Whether ministers made reasonable efforts to obtain information sought by special advocates — Whether ministers breached duties of candour and utmost good faith — Whether proceedings against named person were fair — Whether named person entitled to stay of proceedings.*

H is alleged to have come to Canada for the purpose of engaging in terrorism. In 2002, a security certificate was issued against H under the scheme then contained in the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 (“*IRPA*”). The certificate declared H inadmissible to Canada on national security grounds. After

a successful constitutional challenge of the then existing *IRPA* security certificate scheme and subsequent amendments to the *IRPA*, a second security certificate was issued against H and referred to the Federal Court for a determination as to its reasonableness. During the proceedings, the special advocates appointed to protect the interests of H in the closed hearings sought to obtain disclosure of the identity of human sources who provided information regarding H to the Canadian Security Intelligence Service (“CSIS”) as well as permission to interview and to cross-examine them. The designated judge rejected their request, finding that the common law police informer privilege should be extended to cover CSIS human sources. The designated judge also rejected their request to compel the ministers to obtain updated information from foreign intelligence agencies on several alleged terrorists with whom H was claimed to have associated. In addition, H’s request to exclude from the evidence summaries of intercepted conversations on the ground that the original recordings and notes of these conversations were destroyed pursuant to CSIS policy OPS-217 was refused by the designated judge. The designated judge found the security certificate scheme under the amended *IRPA* to be constitutional, and concluded that the certificate declaring H inadmissible to Canada was reasonable. On appeal, the Federal Court of Appeal upheld the constitutionality of the scheme but found that the identity of CSIS human sources is not protected by privilege. It also excluded from the evidence the summaries of intercepted conversations to which H had not been privy, and remitted the matter to the designated judge for redetermination on the basis of what remained of the record after the exclusion of the summaries.

*Held* (Abella and Cromwell JJ. dissenting in part on the appeal): The appeal should be allowed in part. The cross-appeal should be dismissed. The *IRPA* scheme is constitutional. CSIS human sources are not protected by a class privilege. The designated judge's conclusion that the security certificate was reasonable is reinstated.

*Per McLachlin C.J.* and LeBel, Rothstein, Moldaver, Karakatsanis and Wagner JJ.:

*Constitutionality of IRPA Scheme*

The impugned provisions of the *IRPA* scheme are constitutional. They do not violate the named person's right to know and meet the case against him, or the right to have a decision made on the facts and the law. The alleged defects of the *IRPA* scheme must be assessed in light of the scheme's overall design and of the two central principles that guide the scheme: (1) the designated judge is intended to play a gatekeeper role, is vested with broad discretion and must ensure not only that the record supports the reasonableness of the ministers' finding of inadmissibility but also that the overall process is fair; and (2) participation of the special advocates in closed hearings is intended to be a substantial substitute for personal participation by the named person in those hearings. However, the scheme remains an imperfect substitute for full disclosure in an open court, and the designated judge has an ongoing responsibility to assess the overall fairness of the process and to grant remedies under s. 24(1) of the *Charter* where appropriate.

The *IRPA* scheme provides sufficient disclosure to the named person to be constitutionally compliant, since the designated judge has a statutory duty to ensure that the named person is reasonably informed of the case against him or her throughout the proceedings. However, the *IRPA* scheme's requirement that the named person be "reasonably informed" of the case should be read as a recognition that the named person must receive an incompressible minimum amount of disclosure. A named person is "reasonably informed" if he or she has personally received sufficient disclosure to be able to give meaningful instructions to his public counsel and meaningful guidance and information to his or her special advocates which will allow them to challenge the information and evidence presented in the closed hearings. The level of disclosure required for a named person to be reasonably informed is case-specific, depending on the allegations and evidence against him or her. Ultimately, the designated judge is the arbiter of whether this standard has been met.

Only information and evidence that raises a serious risk of injury to national security or danger to the safety of a person can be withheld from the named person. The designated judge must be vigilant and skeptical with respect to the claims of national security confidentiality and must ensure that only information or evidence which would injure national security or endanger the safety of a person is withheld from the named person. Systematic overclaiming would infringe the named person's right to a fair process or undermine the integrity of the judicial system, requiring a remedy under s. 24(1) of the *Charter*.

The *IRPA* scheme's approach to disclosure, which fails to provide for a balancing of countervailing interests, does not render the scheme unconstitutional. Section 7 of the *Charter* does not require a balancing approach to disclosure, rather, it requires a fair process. Parliament's choice to adopt a categorical prohibition against disclosure of sensitive information, as opposed to a balancing approach, does not as such constitute a breach of the right to a fair process.

The communications restrictions imposed on special advocates do not render the scheme unconstitutional. They are not absolute and can be lifted with judicial authorization, subject to conditions deemed appropriate by the designated judge. The judicial authorization process gives the designated judge a sufficiently broad discretion to allow all communications that are necessary for the special advocates to perform their duties. This broad discretion averts unfairness as the designated judge can ensure that the special advocates function as closely as possible to ordinary counsel in a public hearing. The judge should take a liberal approach in authorizing communications and only refuse authorization where the Minister has demonstrated, on a balance of probabilities, a real risk of injurious disclosure. In addition, the named person and his public counsel can send an unlimited amount of one-way communications to the special advocates at any time throughout the proceedings.

The admission of hearsay evidence or the denial of the opportunity for special advocates to cross-examine sources do not render the *IRPA* scheme

unconstitutional. The *IRPA* scheme achieves the purpose of excluding unreliable evidence by alternative means to the rule against hearsay evidence and the right to cross-examine witnesses – it provides the designated judge with broad discretion to exclude evidence that is not “reliable and appropriate”, which allows the judge to exclude not only evidence that he or she finds, after a searching review, to be unreliable, but also evidence whose probative value is outweighed by its prejudicial effect against the named person.

#### *Privilege for CSIS Human Sources*

CSIS human sources are not protected by a class privilege. First, police informer privilege does not attach to CSIS human sources. The differences between traditional policing and modern intelligence gathering preclude automatically applying traditional police informer privilege to CSIS human sources. While evidence gathered by the police is traditionally used in criminal trials that provide the accused with significant evidentiary safeguards, the intelligence gathered by CSIS may be used to establish criminal conduct in proceedings that have relaxed rules of evidence and allow for the admission of hearsay evidence. Second, this Court should not create a new privilege for CSIS human sources. If Parliament deems it desirable that CSIS human sources’ identities and related information be privileged, it can enact appropriate protections. The *IRPA* scheme already affords broad protection to human sources by precluding the public disclosure of information that would injure national security or endanger a person.

Although the identity of CSIS human sources is not privileged, special advocates do not have an unlimited ability to interview and cross-examine human sources. The discretion of the designated judge to allow the special advocates to interview and cross-examine human sources in a closed hearing should be exercised as a last resort. A generalized practice of calling CSIS human sources before a court, even if only in closed hearings, may have a chilling effect on potential sources and hinder CSIS' ability to recruit new sources. In this case, there is no need to authorize the exceptional measure of interviewing and cross-examining human sources.

### *Summaries*

The appropriate remedy for the destruction of materials pursuant to CSIS policy OPS-217 must be assessed on a case-by-case basis and must be tailored to address the prejudicial effect on the named person's case. The summaries of materials destroyed pursuant to policy OPS-217 should only be excluded under s. 24(1) of the *Charter* if their admission would result in an unfair trial or would otherwise undermine the integrity of the justice system. In this case, the designated judge did not err in refusing to exclude the summaries of intercepted conversations that were tendered as evidence by the ministers. Although the destruction of the original CSIS operational materials caused the ministers to fail to meet their disclosure obligations towards H and therefore to breach s. 7 of the *Charter*, the exclusion of the summaries is not necessary to remedy the prejudice to H's ability to know and meet the case against him, or to safeguard the integrity of the justice

system. The disclosure of the summaries in an abridged version to H and in an unredacted form to his special advocates was sufficient to prevent significant prejudice to H's ability to know and meet the case against him.

#### *Duties of Candour and Utmost Good Faith and Fairness of Process*

The duties of candour and utmost good faith apply when a party relies upon evidence in *ex parte* proceedings. They require an ongoing effort to update, throughout the proceedings, the information and evidence regarding the named person. What constitutes reasonable efforts will turn on the facts of each case, however, the ministers have no general obligation to provide disclosure of evidence or information that is beyond their control. In this case, reasonable efforts were made by the ministers and they did not breach those duties. The proceedings against H were fair and a stay of proceedings should not be granted.

#### *Reasonableness of Certificate*

The designated judge committed no reviewable errors in finding that the ministers' decision to declare H inadmissible to Canada was reasonable. The designated judge's weighing of the factual evidence on the record is entitled to appellate deference and should only be interfered with if he committed a palpable and overriding error. There is no palpable and overriding error in his weighing of the evidence or in his assessment of H's credibility, both of which in his view provided reasonable grounds to establish H's inadmissibility.

*Per Abella and Cromwell JJ.* (dissenting in part on the appeal):  
Individuals who come forward with information about a potential terrorist threat, often risk their lives in doing so if their identity is disclosed. Offering only the possibility of anonymity if a court subsequently agrees to protect an informer's identity, requires informers to choose between risk of personal harm if their identity is not protected, or risk of harm to the public if the information is not disclosed.

CSIS informants who provide national security information based on a promise of confidentiality are entitled to the assurance that their confidentiality will be protected. This can only be guaranteed by a class privilege, as is done in criminal law cases. A case-by-case approach results in an informant not knowing whether the promise will be kept until a judge engages in a retrospective assessment. This is hardly conducive to encouraging informants to risk their lives by coming forward to offer highly sensitive information in terrorism cases.

Informer privilege has been judicially recognized for more than two centuries and has a dual purpose: protection of a channel of information and the safety of those supplying it. It has been applied in settings other than criminal prosecutions, including commissions of inquiry. The privilege for informers in the context of state officials investigating matters of national security is a well-established one. Before CSIS was created as an independent agency, the intelligence function it now carries out was performed by the RCMP Security Service, and informer privilege applied to RCMP Security Service informants. While the

functions of CSIS and the RCMP are distinct, the rationale for the informer privilege applies equally to the work of both. The transfer of functions from the RCMP Security Service to CSIS should have no bearing on whether the privilege continues to exist.

The CSIS informer privilege is not abrogated by statute. In order to abrogate a common law privilege, Parliament must clearly express an intention to do so. *IRPA* makes no reference to informer privilege and does not evince a clear intention to deprive CSIS informants of its benefit.

Given the intensity of the interests at stake in the security certificate context, it would be appropriate to recognize a limited exception specifically crafted for the security certificate process which would address only disclosure to the special advocate, not to the subject of the proceedings. Identity should be disclosed only if the reviewing judge is satisfied that other measures, including withdrawing the substance of the informant's evidence from consideration in support of the certificate, are not sufficient to ensure a just outcome. Even when disclosure of identity is ordered, there should be no cross-examination of the source by the special advocate. Requiring a human source to testify will have a profound chilling effect on the willingness of other sources to come forward, and will undoubtedly damage the relationship between CSIS and the source compelled to testify. CSIS operatives must be able to provide confident assurances to their sources that their identities will not be revealed, not vague assurances hedged with qualifications. Moreover, the human

sources themselves, who are not subject to the necessary security clearance, may learn sensitive material in the closed proceedings which CSIS will then be unable to control.

We would therefore allow the ministers' appeal on the informant privilege issue and restore the designated judge's disposition of this issue.

### **Cases Cited**

By McLachlin C.J.

**Referred to:** *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 S.C.R. 350; *Vancouver Sun (Re)*, 2004 SCC 43, [2004] 2 S.C.R. 332; *Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1996] 3 S.C.R. 480; *Bank Mellat v. H. M. Treasury*, [2013] UKSC 38, [2013] 4 All E.R. 495; *Almrei (Re)*, 2008 FC 1216, [2009] 3 F.C.R. 497; *Ruby v. Canada (Solicitor General)*, 2002 SCC 75, [2002] 4 S.C.R. 3; *R. v. Ahmad*, 2011 SCC 6, [2011] 1 S.C.R. 110; *Secretary of State for the Home Department v. A.F. (No. 3)*, [2009] UKHL 28, [2009] 3 All E.R. 643; *Jaballah, Re*, 2009 FC 279, 340 F.T.R. 43; *Canada (Attorney General) v. Almalki*, 2010 FC 1106, [2012] 2 F.C.R. 508; *Khadr v. Canada (Attorney General)*, 2008 FC 549, 329 F.T.R. 80; *Almrei, Re*, 2009 FC 322, 342 F.T.R. 11; *Smith v. Jones*, [1999] 1 S.C.R. 455; *R. v. L. (D.O.)*, [1993] 4 S.C.R. 419; *R. v. Khelawon*, 2006 SCC 57, [2006] 2 S.C.R. 787; *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326; *R. v. Y. (N.)*, 2012

ONCA 745, 113 O.R. (3d) 347; *R. v. National Post*, 2010 SCC 16, [2010] 1 S.C.R. 477; *Canada (Attorney General) v. Almallki*, 2011 FCA 199, [2012] 2 F.C.R. 594; *R. v. La*, [1997] 2 S.C.R. 680; *R. v. Bjelland*, 2009 SCC 38, [2009] 2 S.C.R. 651; *R. v. Bero* (2000), 137 O.A.C. 336; *R. v. J.G.B.* (2001), 139 O.A.C. 341; *Almrei (Re)*, 2009 FC 1263, [2011] 1 F.C.R. 163; *R. v. Chaplin*, [1995] 1 S.C.R. 727; *R. v. Stinchcombe*, [1995] 1 S.C.R. 754; *R. v. O'Connor*, [1995] 4 S.C.R. 411; *R. v. Babos*, 2014 SCC 16; *Housen v. Nikolaisen*, 2002 SCC 33, [2002] 2 S.C.R. 235.

By Abella and Cromwell JJ. (dissenting in part on the appeal)

*Bisaillon v. Keable*, [1983] 2 S.C.R. 60; *Rice v. National Parole Board* (1985), 16 Admin. L.R. 157; *Wilson v. National Parole Board* (1985), 10 Admin. L.R. 171; *Cadieux v. Director of Mountain Institution*, [1985] 1 F.C. 378; *A. v. Drapeau*, 2012 NBCA 73, 393 N.B.R. (2d) 76; *R. v. Leipert*, [1997] 1 S.C.R. 281; *Named Person v. Vancouver Sun*, 2007 SCC 43, [2007] 3 S.C.R. 253; *R. v. Basi*, 2009 SCC 52, [2009] 3 S.C.R. 389; *R. v. Y. (N.)*, 2012 ONCA 745, 113 O.R. (3d) 347; *Central Intelligence Agency v. Sims*, 471 U.S. 159 (1985); *Solicitor General of Canada v. Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario*, [1981] 2 S.C.R. 494; *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326; *R. v. Ahmad*, 2009 CanLII 84776; *R. v. Debot*, [1989] 2 S.C.R. 1140; *R. v. Garofoli*, [1990] 2 S.C.R. 1421; *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, 2008 SCC 44, [2008] 2 S.C.R. 574.

## Statutes and Regulations Cited

*Act to amend the Immigration and Refugee Protection Act (certificate and special advocate) and to make a consequential amendment to another Act*, S.C. 2008, c. 3.

*Canada Evidence Act*, R.S.C. 1985, c. C-5, ss. 37, 38, 38.06(1), (2).

*Canadian Charter of Rights and Freedoms*, ss. 1, 7, 24(1).

*Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, s. 12.

*Immigration Act*, R.S.C. 1985, c. I-2 [repl. 2001, c. 27].

*Immigration and Refugee Protection Act*, S.C. 2001, c. 27, Part 1, ss. 33, 34, Division 9, 77, 78, 80, 81, 83(1), (1.1), 85.1, 85.2, 85.4, 85.5.

## Authors Cited

Canada. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. First Report. *Security and Information*. Ottawa: The Commission, 1979.

Canada. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. Second Report. *Freedom and Security under the Law*, vols. 1 and 2. Ottawa: The Commission, 1981.

Canada. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. *Report of the Events Relating to Maher Arar: Analysis and Recommendations*. Ottawa: Public Works and Government Services, 2006.

Canada. Parliamentary Research Branch. "The Canadian Security Intelligence Service", Current Issue Review 84-27E, revised January 24, 2000.

Forcese, Craig. "Canada's National Security 'Complex': Assessing the Secrecy Rules" (2009), 15:5 *IRPP Choices* 3.

Forcese, Craig. *National Security Law: Canadian Practice in International Perspective*. Toronto: Irwin Law, 2008.

Forcese, Craig, and Lorne Waldman. "Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of 'Special

Advocates' in National Security Proceedings", August 2007 (online: <http://aix1.uottawa.ca/~cforce/other/sastudy.pdf>).

Paciocco, David M. "When Open Courts Meet Closed Government" (2005), 29 *S.C.L.R.* (2d) 385.

Roach, Kent. "Sources and Trends in Post-9/11 Anti-terrorism Laws", in Benjamin J. Goold and Liora Lazarus, *Security and Human Rights*. Portland, Or.: Hart, 2007, 227.

Roach, Kent. "The eroding distinction between intelligence and evidence in terrorism investigations", in Nicola McGarrity, Andrew Lynch and George Williams, eds., *Counter-Terrorism and Beyond: The Culture of Law and Justice after 9/11*. New York: Routledge, 2010, 48.

Schiff, Stanley. *Evidence in the Litigation Process*, vol. 2, 4th ed. Scarborough, Ont.: Carswell, 1993.

Sedley, Stephen. "Terrorism and Security: Back to the Future?", in David Cole, Federico Fabbrini and Arianna Vidaschi, eds., *Secrecy, National Security and the Vindication of Constitutional Law*. Cheltenham, U.K.: Edward Elgar, 2013, 13.

Stewart, Hamish. *Fundamental Justice: Section 7 of the Canadian Charter of Rights and Freedoms*. Toronto: Irwin Law, 2012.

Wigmore, John Henry. *Evidence in Trials at Common Law*, vol. 8. Revised by John T. McNaughton. Boston: Little, Brown, 1961.

APPEAL and CROSS-APPEAL from a judgment of the Federal Court of Appeal (Blais C.J. and Létourneau and Layden-Stevenson JJ.A.), 2012 FCA 122, [2012] 3 F.C.R. 635, 349 D.L.R. (4th) 519, 7 Imm. L.R. (4th) 175, 429 N.R. 1, 260 C.R.R. (2d) 290, [2012] F.C.J. No. 492 (QL), 2012 CarswellNat 1155, setting aside three decisions of Noël J., 2009 FC 204, [2009] 4 F.C.R. 370, 339 F.T.R. 65, 306 D.L.R. (4th) 269, 78 Imm. L.R. (3d) 303, [2008] F.C.J. No. 1823 (QL), 2008 CarswellNat 5335; 2010 FC 1241, [2012] 3 F.C.R. 251, 380 F.T.R. 61, [2010] F.C.J. No. 1426 (QL), 2010 CarswellNat 4699; and 2010 FC 1243, 380 F.T.R. 255, 224

C.R.R. (2d) 167, 95 Imm. L.R. (3d) 1, [2010] F.C.J. No. 1428 (QL), 2010 CarswellNat 5848; and affirming a decision of Noël J., 2010 FC 1242, [2012] 3 F.C.R. 432, 380 F.T.R. 163, 224 C.R.R. (2d) 93, 94 Imm. L.R. (3d) 179, [2010] F.C.J. No. 1427 (QL), 2010 CarswellNat 4714. Appeal allowed in part, Abella and Cromwell JJ. dissenting in part. Cross-appeal dismissed.

*Urszula Kaczmarczyk, Q.C., Robert Frater, Marianne Zoric and André Séguin*, for the appellants/respondents on cross-appeal.

*Matthew C. Webber, Norman D. Boxall, Meaghan Thomas and Leo Russomanno*, for the respondent/appellant on cross-appeal.

*Robert W. Hubbard and Greg Skerkowski*, for the intervener the Attorney General of Ontario.

*Nader R. Hasan and Gerald Chan*, for the intervener the British Columbia Civil Liberties Association.

*John Norris and François Dadour*, for the intervener the Canadian Council of Criminal Defence Lawyers.

*Anil K. Kapoor and Lindsay Trevelyan*, for the intervener the Canadian Civil Liberties Association.

*Lorne Waldman, Peter Edelmann, Jacqueline Swaisland and Clare Crummey*, for the intervener the Canadian Bar Association.

*Marlys A. Edwardh and Adriel Weaver*, for the intervener the Canadian Association of Refugee Lawyers.

*Barbara Jackman, Sharryn J. Aiken and Andrew J. Brouwer*, for the interveners the Canadian Council for Refugees and the International Civil Liberties Monitoring Group.

*Faisal Bhabha and Khalid M. Elgazzar*, for the intervener the Canadian Council on American-Islamic Relations (now known as National Council of Canadian Muslims).

*Michael Bossin, Laïla Demirdache and Anna Shea*, for the intervener Amnesty International.

*Breese Davies and Erin Dann*, for the intervener the Criminal Lawyers' Association (Ontario).

*Paul J. J. Cavalluzzo and Paul D. Copeland*, as Special Advocates.

The judgment of McLachlin C.J. and LeBel, Rothstein, Moldaver, Karakatsanis and Wagner JJ. was delivered by

THE CHIEF JUSTICE —

[1] The Minister of Citizenship and Immigration and the Minister of Public Safety and Emergency Preparedness (collectively, “the ministers”) seek to have Mohamed Harkat, a non-citizen, declared inadmissible to Canada. Mr. Harkat is alleged to have come to Canada for the purpose of engaging in terrorism. He has been detained, or living under strict conditions, for over a decade. He potentially faces deportation to a country where he may be at risk of torture or death, although the constitutionality of his deportation in such circumstances is not before us in the present appeal.

[2] The reasonableness of the ministers’ decision to declare Mr. Harkat inadmissible to Canada is subject to judicial review, under Division 9 of Part 1 of the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 (the “*IRPA* scheme”). This scheme prevents Mr. Harkat from seeing some of the evidence and information tendered against him, because its public disclosure would harm national security.

[3] The issue in this appeal is whether the *IRPA* scheme complies with the Constitution, in particular the guarantee in the *Canadian Charter of Rights and Freedoms* against unjustifiable intrusions on life, liberty, and security of the person. More specifically, this appeal asks whether the *IRPA* scheme gives Mr. Harkat a fair

opportunity to defend himself against the allegations made by the ministers, despite the fact that national security considerations prevent him from seeing the entire record and from personally participating in all of the hearings. It requires us to determine how far the principle of full disclosure in an open court can be qualified in order to address the threat posed by non-citizens who may be involved in terrorism.

[4] I conclude that that the *IRPA* scheme is constitutional. Crafting a regime that achieves a fundamentally fair process while protecting confidential national security information is a difficult task. The scheme must apply to a broad range of cases, implicating a variety of national security concerns. Parliament's response to this challenge has been to confer on judges the discretion and flexibility to fashion a fair process, in the particular case before them. If this is impossible, judges must not hesitate to find a breach of the right to a fair process and to grant whatever remedies are appropriate, including a stay of proceedings.

[5] In the present case, the process was fair and the Federal Court judge committed no reviewable errors in finding that the ministers' decision to declare Mr. Harkat inadmissible to Canada was reasonable.

#### History of the Legislation and of the Proceedings

##### *The Legislation*

[6] The purpose of the *IRPA* scheme “is to permit the removal of non-citizens living in Canada — permanent residents and foreign nationals — on various grounds, including connection with terrorist activities”: *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 S.C.R. 350 (“*Charkaoui I*”), at para. 4. The ministers must decide whether the evidence against a non-citizen gives them reasonable grounds to declare him or her “inadmissible” to Canada — i.e. to issue a removal order. The resulting “certificate of inadmissibility” (also called a “security certificate”) is then referred to the Federal Court for a review of its reasonableness. If a Federal Court judge (the “designated judge”) finds the certificate to be reasonable, the non-citizen named in that certificate (the “named person”) becomes subject to a removal order.

[7] The *IRPA* scheme was adopted by Parliament in 2001, as a successor to an analogous scheme contained in the *Immigration Act*, R.S.C. 1985, c. I-2. In the wake of the attacks of September 11, 2001, it increasingly came to be used as a means of detaining suspected terrorists and eliminating the perceived threat posed by them: K. Roach, “*Sources and Trends in Post-9/11 Anti-Terrorism Laws*”, in B.J. Goold and L. Lazarus, *Security and Human Rights* (2007), 227, at p. 233. From a practical perspective, the *IRPA* scheme is in some respects more advantageous for the state than criminal proceedings. It has a lower standard of proof and is more protective of confidential national security information than the criminal law: *ibid.* As will be discussed further below, any information that would be injurious to national security or to the safety of any person is not disclosed to the named person. This information

can nevertheless be presented to the designated judge in closed hearings and relied upon by her in assessing the security certificate's reasonableness.

[8] The constitutionality of the *IRPA* scheme was challenged by Mr. Harkat and other non-citizens named in security certificates. In *Charkaoui I*, this Court found that the *IRPA* scheme deprived named persons of their life, liberty, and security of the person in a manner that was not in accordance with principles of fundamental justice, contrary to s. 7 of the *Charter*. It found that the *IRPA* scheme precluded the judge from making a decision based on all the relevant facts and law, because it did not provide for representation of the named person in the closed portion of the proceedings. It also held that the *IRPA* scheme violated the principle that a person must have the ability to know and meet the case against him, because there was not full disclosure of the government's case to the named person or any substantial substitute for full disclosure.

[9] The Court concluded that these breaches could not be justified under s. 1 of the *Charter*, because the *IRPA* scheme did not minimally impair the named person's rights. Other types of closed proceedings, both in Canada and abroad, accomplished the goal of protecting confidential national security information less intrusively. For example, in the United Kingdom, special advocates were appointed to receive disclosure on an appellant's behalf and to defend his or her interests in closed hearings before the Special Immigration Appeals Commission. These special advocates were bound not to reveal confidential information to anyone or (subject to

narrow exceptions) to communicate with the appellant. While that system was not without its drawbacks, this Court concluded that, “without compromising security, it better protects the named person’s s. 7 interests”: *Charkaoui I*, at para. 86.

[10] In response to this Court’s ruling, Parliament made several amendments to the *IRPA* scheme: *An Act to amend the Immigration and Refugee Protection Act (certificate and special advocate) and to make a consequential amendment to another Act*, S.C. 2008, c. 3; the amended *IRPA* scheme is reproduced in the Appendix to these reasons. In particular, it created a role for special advocates, who protect the interests of the named person in closed hearings after having received disclosure of the entire record.

### *The Proceedings*

[11] In 2002, the Solicitor General of Canada and the Minister of Citizenship and Immigration issued a first security certificate declaring Mr. Harkat inadmissible to Canada on national security grounds. After the successful constitutional challenge and the amendment of the *IRPA* scheme, the ministers issued a second security certificate against Mr. Harkat and commenced new proceedings before the Federal Court.

[12] Disclosure issues arose during the proceedings with respect to the individuals (the “human sources”) who secretly provided information regarding Mr. Harkat to the Canadian Security Intelligence Service (“CSIS”). The special advocates

sought to obtain disclosure of the identity of the CSIS human sources, as well as permission to interview and to cross-examine them in a closed hearing. Noël J. rejected this request. He reasoned that the common law police informer privilege, which is a rule against the disclosure of any information that might identify a police informer, should be extended to cover CSIS human sources: 2009 FC 204, [2009] 4 F.C.R. 370.

[13] At a later point during the disclosure process, it was discovered that the judge and the special advocates had been provided with an incomplete and misleading document regarding one of the CSIS human sources. The document provided to Mr. Harkat's special advocates failed to disclose that a 2002 polygraph test conducted on the relevant source initially revealed him or her to be untruthful. As a remedy, Noël J. ordered the disclosure of unredacted human source files to the special advocates: 2009 FC 553, 345 F.T.R. 143; 2009 FC 1050, [2010] 4 F.C.R. 149.

[14] The special advocates also sought to compel the ministers to obtain updated information from foreign intelligence agencies on several alleged terrorists with whom Mr. Harkat was claimed to have associated. They were ultimately dissatisfied with the efforts undertaken by the ministers and sought a stay of proceedings. Noël J. rejected this request, finding that the ministers took reasonable steps to get updated information from foreign intelligence agencies: 2010 FC 1243, 380 F.T.R. 255, at Annex "A".

[15] Mr. Harkat also sought to have the summaries of intercepted conversations excluded from the evidence on the ground that the original recordings and notes of these conversations, in which he allegedly participated or in which he was allegedly a subject of conversation, were destroyed pursuant to CSIS policy OPS-217. Alternatively, he sought a stay of proceedings in consideration of a number of breaches. Noël J. found that Mr. Harkat suffered no prejudice from the destruction of those original operational materials: 2010 FC 1243. He reasoned that the summaries of the conversations were prepared in a way that ensured their accuracy, and that they were corroborated by the overall narrative about Mr. Harkat which emerged during the hearings. Consequently, he refused to exclude them from the evidence against Mr. Harkat.

[16] Finally, Mr. Harkat challenged the constitutionality of the amended *IRPA* scheme. Noël J. found the regime to be constitutional: 2010 FC 1242. In his view, the special advocates provided a substantial substitute for full disclosure to Mr. Harkat and vigorously defended his interests during the closed portion of the proceedings.

[17] After consideration of evidence tendered in both public and closed hearings, Noël J. came to the conclusion that the certificate declaring Mr. Harkat inadmissible to Canada was reasonable: 2010 FC 1241. He made adverse findings of credibility against Mr. Harkat and found that the evidence provided reasonable grounds to believe that Mr. Harkat had been involved with terrorist organizations. He

held that Mr. Harkat's behaviour and lies were consistent with the theory that he had come to Canada as a "sleeper" agent for terrorist organizations.

[18] Mr. Harkat appealed Noël J.'s conclusions. The Federal Court of Appeal (*per* Létourneau J.A.) allowed the appeal in part: 2012 FCA 122, [2012] 3 F.C.R. 635. It agreed with Noël J.'s conclusion that the amended *IRPA* scheme is constitutional. However, it found that the identity of CSIS human sources is not protected by privilege. It also excluded from the evidence the summaries of intercepted conversations to which Mr. Harkat had not been privy. It remitted the matter to Noël J. for redetermination on the basis of what remained of the record after the exclusion of the summaries.

### Issues

[19] The ministers appeal to this Court, seeking the reinstatement of Noël J.'s conclusion that the security certificate was reasonable. They also ask for recognition of the CSIS human source privilege.

[20] Mr. Harkat cross-appeals. He asks this Court to find the amended *IRPA* scheme unconstitutional. Alternatively, he seeks a new reasonableness hearing before a new designated judge, the exclusion of the summaries of all the intercepted conversations for which the original CSIS operational materials were destroyed, and permission for his special advocates to interview and cross-examine the human sources. He also takes issue with Noël J.'s weighing of "open source" evidence (such

as books on terrorism and publications in political science periodicals), which led him to conclude that the individuals with whom Mr. Harkat associated were members of terrorist organizations.

[21] In addition, the special advocates contest Noël J.'s refusal to order a stay of proceedings. They contend that the ministers breached their duties of candour and utmost good faith, and that the proceedings did not allow them to meaningfully test the case brought against Mr. Harkat.

[22] This appeal raises the following issues:

- A. Does the *IRPA* scheme violate the *Charter*?
- B. Are CSIS human sources covered by privilege and can they be cross-examined?
- C. Did the designated judge err in refusing to exclude the summaries of intercepted conversations?
- D. Did the ministers breach their duties of candour and utmost good faith?
- E. Were the proceedings against Mr. Harkat fair?

F. Did the designated judge err in concluding that the security certificate was reasonable?

### Analysis

#### *Preliminary Comment*

[23] At the request of the ministers, this Court conducted two distinct hearings on this appeal. One was open to the public, while the second was held behind closed doors. Having heard the confidential submissions, it is my view that it was unnecessary to conduct a portion of the appeal hearing behind closed doors.

[24] The open court principle is “a hallmark of a democratic society and applies to all judicial proceedings”: *Vancouver Sun (Re)*, 2004 SCC 43, [2004] 2 S.C.R. 332, at para. 23; see also D. M. Paciocco, “When Open Courts Meet Closed Government” (2005), 29 *S.C.L.R.* (2d) 385, at pp. 391-95; *Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1996] 3 S.C.R. 480, at para. 20. “National security does not negate the open court principle”: C. Forcese, *National Security Law: Canadian Practice in International Perspective* (2008), at p. 402. The Supreme Court of the United Kingdom recently commented unfavourably on a hearing that it held behind closed doors at the request of the government, which had raised national security concerns: *Bank Mellat v. H. M. Treasury*, [2013] UKSC 38, [2013] 4 All E.R. 495, at para. 60, *per* Lord Neuberger P.S.C. It noted that closed evidence is factual in nature, whereas the points debated before appellate courts are

essentially legal: *ibid.*. Consequently, the Supreme Court found that closed hearings before it would rarely, if ever, be necessary for the proper disposition of an appeal.

[25] The issues in this appeal do not turn on confidential information and could have been debated fully in public without any serious risk of disclosure, supplemented where necessary by brief closed written submissions and by the closed record. The special advocates could have been given judicial permission to make public submissions, so long as they refrained from disclosing confidential information: see s. 85.4(2) and (3) of the *Immigration and Refugee Protection Act* (“*IRPA*”).

[26] The content of the closed hearing overlapped significantly with the open hearing and did not assist this Court in deciding the issues before it. It served only to foster an appearance of opacity of these proceedings, which runs contrary to the fundamental principles of transparency and accountability.

[27] I now turn to the issues on appeal.

*Does the IRPA Scheme Violate the Charter?*

[28] Mr. Harkat and his special advocates contend that the *IRPA* scheme fails to provide a fair process to the named person, as required by s. 7 of the *Charter*. They argue that the regime is unconstitutional because it provides insufficient disclosure to

the named person, does not allow the special advocates to communicate freely with the named person, and allows for the admission of hearsay evidence.

[29] After providing a brief overview of the *IRPA* scheme, I will address in turn Mr. Harkat's rights under s. 7 of the *Charter*, the principles that guide the scheme, and the scheme's alleged defects.

### Overview of the *IRPA* Scheme

#### *Commencement of Proceedings*

[30] A security certificate may be issued by the ministers for the removal from Canada of a non-citizen (whether a permanent resident or a foreign national) who is inadmissible on security grounds. The grounds for inadmissibility include engaging in terrorism, being a danger to the security of Canada, engaging in acts of violence that would or might endanger the lives or safety of persons in Canada, or being a member of an organization that engages in terrorism: s. 34, *IRPA*. The ministers must have reasonable grounds to believe that the facts giving rise to inadmissibility have occurred, are occurring, or may occur: s. 33, *IRPA*.

[31] As a practical matter, the process commences when CSIS presents a Security Intelligence Report ("SIR") to the ministers. The SIR sets out in detail the allegations and evidence grounding inadmissibility. If the ministers conclude that the allegations in the SIR are reasonably grounded, they issue a security certificate.

[32] Once the certificate is issued, the ministers must refer it to the Federal Court: s. 77(1), *IRPA*. The Federal Court judge who is designated to hear the case “shall determine whether the certificate is reasonable and shall quash the certificate if he or she determines that it is not”: s. 78, *IRPA*. If the designated judge deems the certificate to be reasonable, the named person is inadmissible and the certificate becomes a removal order in force: s. 80, *IRPA*. The named person may be arrested and detained for the duration of the proceedings before the Federal Court: s. 81, *IRPA*.

#### *The Disclosure of Summaries to the Named Person*

[33] The named person must be given summaries of the information and evidence which allow him to be reasonably informed of the case against him: ss. 77(2) and 83(1)(e), *IRPA*. The summaries must “not include anything that, in the judge’s opinion, would be injurious to national security or endanger the safety of any person if disclosed”: s. 83(1)(e), *IRPA*.

#### *Special Advocates*

[34] The judge must appoint one or more special advocates to protect the interests of the named person in closed hearings: s. 83(1)(b), *IRPA*. These hearings are held *in camera* and *ex parte*, in order to permit the Minister to present information and evidence the public disclosure of which could be injurious to national security or endanger the safety of a person: s. 83(1)(c), *IRPA*.

[35] Special advocates are security-cleared lawyers whose role is to protect the interests of the named person and “to make up so far as possible for the [named person’s] own exclusion from the evidentiary process”: S. Sedley, “Terrorism and Security: Back to the Future?”, in D. Cole, F. Fabbrini and A. Vidaschi, eds., *Secrecy, National Security and the Vindication of Constitutional Law* (2013), 13, at p. 16. During the closed hearings, they perform the functions that the named person’s counsel (the “public counsel”) performs in the open hearings. They do so by challenging the Minister’s claims that information or evidence should not be disclosed, and by testing the relevance, reliability, and sufficiency of the secret evidence: s. 85.1(1) and (2), *IRPA*. They are active participants in the closed hearings. They may make submissions and cross-examine witnesses who appear in those hearings: s. 85.2(a) and (b), *IRPA*. The *IRPA* scheme also provides that the special advocates may “exercise, with the judge’s authorization, any other powers that are necessary to protect the interests” of the named person: s. 85.2(c), *IRPA*.

[36] No solicitor-client relationship exists between the special advocates and the named person: s. 85.1(3), *IRPA*. However, solicitor-client privilege is deemed to apply to exchanges between the special advocates and the named person, provided that those exchanges would attract solicitor-client privilege at common law: s. 85.1(4), *IRPA*. As Lutfy C.J. put it, “[a]s between special advocates and named persons, Division 9 protects information and not relationships. . . . The information that passes between them, absent the solicitor and client relationship, is deemed to be protected”: *Almrei (Re)*, 2008 FC 1216, [2009] 3 F.C.R. 497, at paras. 56-57.

[37] Strict communication rules apply to special advocates, in order to prevent the inadvertent disclosure of sensitive information. After the special advocates are provided with the confidential information and evidence, they “may, during the remainder of the proceeding, communicate with another person about the proceeding only with the judge’s authorization and subject to any conditions that the judge considers appropriate”: s. 85.4(2), *IRPA*. Read plainly, “this prohibition covers all information about the proceeding from both public and private sessions, including any testimony given in the absence of the public and the named person and their counsel”: *Almrei*, at para. 16. By contrast, any other person — such as the ministers’ counsel or the court personnel in attendance at closed hearings — is subject to significantly fewer restrictions on communication. Other persons must refrain from communicating about the proceedings only (i) if that person has had a court-authorized communication with the special advocates and the judge has specifically prohibited that person from communicating with anyone else about the proceeding, or (ii) if the communication would disclose the content of a closed hearing: ss. 85.4(3), 85.5(a) and (b), *IRPA*.

#### *Admissibility of Evidence*

[38] The usual rules of evidence do not apply to the proceedings. Instead, “the judge may receive into evidence anything that, in the judge’s opinion, is reliable and appropriate, even if it is inadmissible in a court of law, and may base a decision on that evidence”: s. 83(1)(h), *IRPA*.

[39] The *IRPA* scheme provides that the judge's decision can be based on information or evidence that is not disclosed in summary form to the named person: s. 83(1)(i). It does not specify expressly whether a decision can be based in whole, or only in part, on information and evidence that is not disclosed to the named person.

#### The Section 7 Charter Right to a Fair Process

[40] In *Charkaoui I*, this Court found that the *IRPA* scheme engages significant life, liberty, and security of the person interests: paras. 12-16. Laws that interfere with these interests must conform to the principles of fundamental justice. If they fail to do so, they breach s. 7 of the *Charter* and fail to be justified under s. 1 of the *Charter*.

[41] Pursuant to the principles of fundamental justice, a named person must be provided with a fair process: *Charkaoui I*, at paras. 19-20. At issue in the present appeal are two interrelated aspects of the right to a fair process: the right to know and meet the case, and the right to have a decision made by the judge on the facts and the law. The named person must "be informed of the case against him or her, and be permitted to respond to that case": *Charkaoui I*, at para. 53. Correlatively, the named person's knowledge of the case and participation in the process must be sufficient to result in the designated judge being "exposed to the whole factual picture" of the case and having the ability to apply the relevant law to those facts: *ibid.*, at para. 51.

[42] This said, the assessment of whether a process is fair must take into account the legitimate need to protect information and evidence that is critical to national security. As I wrote in *Charkaoui I*, “[i]nformation may be obtained from other countries or from informers on condition that it not be disclosed. Or it may simply be so critical that it cannot be disclosed without risking public security”: para. 61.

[43] Full disclosure of information and evidence to the named person may be impossible. However, the basic requirements of procedural justice must be met “in an alternative fashion appropriate to the context, having regard to the government’s objective and the interests of the person affected”: *Charkaoui I*, at para. 63. The alternative proceedings must constitute a substantial substitute to full disclosure. Procedural fairness does not require a perfect process — there is necessarily some give and take inherent in fashioning a process that accommodates national security concerns: *Ruby v. Canada (Solicitor General)*, 2002 SCC 75, [2002] 4 S.C.R. 3, at para. 46.

[44] The overarching question, therefore, is whether the amended *IRPA* scheme provides a named person with a fair process, taking into account the imperative of protecting confidential national security information.

#### The Guiding Principles of the *IRPA* Scheme

[45] The alleged defects in the *IRPA* scheme must be assessed in light of the scheme's overall design. Two central principles guide the scheme.

[46] First, the designated judge is intended to play a gatekeeper role. The judge is vested with broad discretion and must ensure not only that the record supports the reasonableness of the ministers' finding of inadmissibility, but also that the overall process is fair: "[I]n a special advocate system, an unusual burden will continue to fall on judges to respond to the absence of the named person by pressing the government side more vigorously than might otherwise be the case": C. Forcese and L. Waldman, "Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of "Special Advocates" in National Security Proceedings" (2007) (online), at p. 60. Indeed, the *IRPA* scheme expressly requires the judge to take into account "considerations of fairness and natural justice" when conducting the proceedings: s. 83(1)(a), *IRPA*. The designated judge must take an interventionist approach, while stopping short of assuming an inquisitorial role.

[47] Second, participation of the special advocates in closed hearings is intended to be a substantial substitute for personal participation by the named person in those hearings. With respect to the confidential portion of the case against the named person, the special advocates must be in a position to act as vigorously and effectively as the named person himself would act in a public proceeding. Indeed, Parliament added special advocates as a feature of the *IRPA* scheme in order to bring it into compliance with the substantive requirements of s. 7 of the *Charter*, as

articulated in *Charkaoui I*. Whether the scheme allows for this intention to become a reality is the central constitutional issue in this appeal, to which I now turn.

#### The Alleged Shortfalls of the IRPA Scheme

[48] In essence, Mr. Harkat alleges that the disclosure of public summaries and the representation of the interests of the named person by special advocates do not suffice to bring the *IRPA* scheme into compliance with the requirements of s. 7 of the *Charter*. I will address each of the alleged defects of the scheme in turn.

#### *Does the Scheme Provide the Named Person With Sufficient Disclosure?*

[49] Mr. Harkat contends that the public summaries of the closed record are too vague and general. In his view, they do not allow a named person to know and meet the case against him or her. He argues that the essence of the right to know and meet a case is the ability to meet detail with detail. He also contends that the *IRPA* scheme takes too categorical an approach to disclosure: a named person will *never* obtain disclosure of information which would be injurious to national security or to the safety of any person, regardless of the importance of disclosure to the named person's case. A less rights-impairing alternative would be a balancing approach such as the one found in s. 38.06(2) of the *Canada Evidence Act*, R.S.C. 1985, c. C-5 ("CEA"), which permits the public interest in non-disclosure to be balanced against the public interest in disclosure.

[50] In my view, the *IRPA* scheme provides sufficient disclosure to the named person to be constitutionally compliant. I base this conclusion on the designated judge's statutory duty to ensure that the named person is reasonably informed of the Minister's case throughout the proceedings.

The *IRPA* Scheme Requires an Incompressible Minimum Amount of Disclosure to the Named Person

[51] At first blush, the provisions of the *IRPA* scheme appear to give precedence to confidentiality of information over the named person's right to know and meet the case. Section 83(1)(e) provides that,

throughout the proceeding, the judge shall ensure that the permanent resident or foreign national is provided with a summary of information and other evidence that enables them to be reasonably informed of the case made by the Minister in the proceeding but that does not include anything that, in the judge's opinion, would be injurious to national security or endanger the safety of any person if disclosed;

Thus, the content of the summaries must be tailored to satisfy the overriding proviso that no information or evidence injurious to national security or to the safety of any person may be disclosed.

[52] The *IRPA* scheme also provides, at s. 83(1)(i), that the judge may base his decision on information or evidence of which the named person has not been informed in summary form: "[T]he judge may base a decision on information or other

evidence even if a summary of that information or other evidence is not provided to the permanent resident or foreign national ...”.

[53] The combination of ss. 83(1)(e) and 83(1)(i) could conceivably lead to a situation where the judge makes a decision on the reasonableness of the security certificate despite the fact that the named person has only received severely truncated disclosure. Noël J. even contemplated a scenario where the named person receives virtually no disclosure: “There may come a time when the only evidence to justify inadmissibility on security ground originates from a very sensitive source, and that the disclosure of such evidence, even through a summary, would inevitably disclose the source” (2010 FC 1242, at para. 59). He nevertheless found the disclosure provisions of the *IRPA* scheme to be constitutional.

[54] In my view, Noël J. erred in interpreting the *IRPA* scheme in a manner that allows for that scenario. *Charkaoui I* makes clear that there is an incompressible minimum amount of disclosure that the named person must receive in order for the scheme to comply with s. 7 of the *Charter*. He or she must receive sufficient disclosure to know and meet the case against him or her.

[55] Parliament amended the *IRPA* scheme with the intent of making it compliant with the s. 7 requirements expounded in *Charkaoui I*, and it should be interpreted in light of this intention: *R. v. Ahmad*, 2011 SCC 6, [2011] 1 S.C.R. 110, at paras. 28-29. The *IRPA* scheme’s requirement that the named person be “reasonably informed” (“*suffisamment informé*”) of the Minister’s case should be

read as a recognition that the named person must receive an incompressible minimum amount of disclosure.

[56] Under the *IRPA* scheme, a named person is “reasonably informed” if he has personally received sufficient disclosure to be able to give meaningful instructions to his public counsel and meaningful guidance and information to his special advocates which will allow them to challenge the information and evidence relied upon by the Minister in the closed hearings. Indeed, the named person’s ability to answer the Minister’s case hinges on the effectiveness of the special advocates, which in turn depends on the special advocates being provided with meaningful guidance and information. As the House of Lords of the United Kingdom put it in referring to disclosure under the British special advocates regime, the named person

must be given sufficient information about the allegations against him to enable him to give effective instructions in relation to those allegations. . . . Where . . . the open material consists purely of general assertions and the case . . . is based solely or to a decisive degree on closed materials the requirements of a fair trial will not be satisfied, however cogent the case based on the closed materials may be.

*(Secretary of State for the Home Department v. A.F. (No. 3), [2009] UKHL 28, [2009] 3 All E.R. 643, at para. 59, per Lord Phillips of Worth Matravers)*

I would add that the named person need not only be given sufficient information about the allegations against him, but also about the evidence on the record.

[57] The level of disclosure required for a named person to be reasonably informed is case-specific, depending on the allegations and evidence against the named person. Ultimately, the judge is the arbiter of whether this standard has been met. At the very least, the named person must know the essence of the information and evidence supporting the allegations. This excludes the scenario where the named person receives no disclosure whatsoever of essential information or evidence.

[58] The *IRPA* scheme is silent as to what happens if there is an irreconcilable tension between the requirement that the named person be “reasonably informed”, on the one hand, and the imperative that sensitive information not be disclosed, on the other. The *IRPA* scheme does not provide that the “reasonably informed” standard can be compromised. But nor does it provide that sensitive information can be disclosed where this is absolutely necessary in order for the “reasonably informed” standard to be met.

[59] In my view, the necessary outcome of situations where there is an irreconcilable tension is that the Minister must withdraw the information or evidence whose non-disclosure prevents the named person from being reasonably informed. In some cases, this may effectively compel the Minister to put an end to the proceedings.

[60] To hold that the Minister can rely on essential information and evidence of which the named person cannot be reasonably informed would force the judge to violate the responsibility expressly placed on him by the statute, i.e. his duty to ensure that the named person remain reasonably informed throughout the proceedings. It

cannot have been Parliament's intent to design a scheme in which the judge is required to violate the responsibilities placed upon him. Consequently, the *IRPA* scheme must be interpreted as precluding the Minister from bringing a case in respect of which the named person cannot be kept reasonably informed. The scheme mandates that the named person remain reasonably informed — i.e. that he be able to give meaningful instructions to his public counsel and meaningful guidance and information to his special advocates — throughout the proceedings. If the named person is not reasonably informed, the proceedings will not have been in compliance with the *IRPA* scheme and the judge cannot confirm the certificate's reasonableness. In such a case, the judge must quash the certificate, pursuant to s. 78 of the *IRPA*.

Only Information or Evidence That Raises a Serious Risk Must Be Withheld

[61] Only information and evidence that raises a *serious* risk of injury to national security or danger to the safety of a person can be withheld from the named person. The judge must ensure throughout the proceedings that the Minister does not cast too wide a net with his claims of confidentiality.

[62] While the *IRPA* scheme provides that closed hearings must be held when the disclosure of information *could* be injurious (s. 83(1)(c), *IRPA*), it mandates the withholding of information from public summaries only if its disclosure *would, in the judge's opinion*, be injurious (s. 83(1)(e), *IRPA*). The judge must err on the side of caution in ordering closed hearings during which he can ascertain the validity of the

Minister's position with respect to the sensitivity of given information or evidence. However, once the judge has heard the parties, he must ensure that only information or evidence which *would* injure national security or endanger the safety of a person is withheld from the named person. "It is the Ministers who bear the burden of establishing that disclosure not only could but would be injurious to national security, or endanger the safety of any person": *Jaballah, Re*, 2009 FC 279, 340 F.T.R. 43, at para. 9, *per* Dawson J. (emphasis added).

[63] The judge must be vigilant and skeptical with respect to the Minister's claims of confidentiality. Courts have commented on the government's tendency to exaggerate claims of national security confidentiality: *Canada (Attorney General) v. Almalki*, 2010 FC 1106, [2012] 2 F.C.R. 508, at para. 108, ; *Khadr v. Canada (Attorney General)*, 2008 FC 549, 329 F.T.R. 80, at paras. 73-77 and 98; see generally C. Forcese, "Canada's National Security 'Complex': Assessing the Secrecy Rules" (2009), 15:5 *IRPP Choices* 3. As Justice O'Connor commented in his report on the Arar inquiry,

overclaiming exacerbates the transparency and procedural fairness problems that inevitably accompany any proceeding that can not be fully open because of [national security confidentiality] concerns. It also promotes public suspicion and cynicism about legitimate claims by the Government of national security confidentiality.

(Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), at p. 302)

[64] The judge is the gatekeeper against this type of overclaiming, which undermines the *IRPA* scheme's fragile equilibrium. Systematic overclaiming would infringe the named person's right to a fair process or undermine the integrity of the judicial system, requiring a remedy under s. 24(1) of the *Charter*.

The Absence of a Balancing Approach Does Not Make the Scheme  
Unconstitutional

[65] In addition, Mr. Harkat argues that the *IRPA* scheme's approach to disclosure is unconstitutional because it fails to provide for a balancing of countervailing interests. In his view, s. 7 of the *Charter* requires the adoption of an approach similar to the one found in s. 38.06(2) of the *CEA*, which allows the judge to order disclosure of national security information if "the public interest in disclosure outweighs in importance the public interest in non-disclosure".

[66] I would reject this contention. Section 7 of the *Charter* does not require a balancing approach to disclosure. Rather, it requires a fair process. "There is no free-standing principle of fundamental justice requiring a proper balancing of interests in general, or requiring the balancing of interests in decisions about disclosure": H. Stewart, *Fundamental Justice: Section 7 of the Canadian Charter of Rights and Freedoms* (2012), at p. 229. Parliament's choice to adopt a categorical prohibition against disclosure of sensitive information, as opposed to a balancing approach, does not as such constitute a breach of the right to a fair process.

*Are the Special Advocates a “Substantial Substitute” to Participation by the Named Person?*

[67] As discussed, the named person and his public counsel do not have access to the closed record, nor can they participate in the closed hearings. Parliament added the role of special advocates to the *IRPA* scheme so that they could serve as a proxy for the named person in the closed portion of the proceedings. Mr. Harkat argues that the restrictions on the special advocates’ ability to communicate with the named person prevent them from effectively protecting the named person’s interests. Specifically, he claims that communications between the named person and the special advocates should not be subject to restrictions. He also contends that the special advocates will be unable to seek judicial authorization without breaching solicitor-client privilege. As a consequence, in his view, the addition of special advocates to the regime fails to address the concerns voiced by this Court in *Charkaoui I*.

[68] The communications restrictions imposed on special advocates are significant, requiring judicial authorization for *any* communication regarding the proceedings between the special advocates and the named person or a third party, after the special advocates have received confidential materials. However, they do not render the scheme unconstitutional. I come to this conclusion for three reasons.

[69] First, the restrictions on communications by the special advocates are not absolute. They can be lifted with judicial authorization, subject to conditions deemed

appropriate by the designated judge: s. 85.4(2), *IRPA*. While this process is less fluid and efficient than the unfettered communications that prevail between a lawyer and his client, it should be remembered that s. 7 of the *Charter* does not guarantee a perfect process. The judicial authorization process gives the designated judge a sufficiently broad discretion to allow all communications that are necessary for the special advocates to perform their duties.

[70] The broad discretion conferred by the *IRPA* scheme averts unfairness that might otherwise result from the communications restrictions. The designated judge can ensure that the special advocates function as closely as possible to ordinary counsel in a public hearing. The restrictions on communications are designed to avert *serious* risks of disclosure of information or evidence whose disclosure would be injurious to national security or to the safety of any person. While the *IRPA* scheme requires the judge to minimize risks of inadvertent disclosure of information, the judge must also give special advocates significant latitude. The special advocates are competent and security-cleared lawyers, who take their professional and statutory obligations seriously. They have the ability to distinguish between the public and confidential aspects of their case. The judge should take a liberal approach in authorizing communications and only refuse authorization where the Minister has demonstrated, on a balance of probabilities, a real — as opposed to a speculative — risk of injurious disclosure. As much as possible, the special advocates should be allowed to investigate the case and develop their strategy by communicating with the

named person, the named person's public counsel, and third parties who may bring relevant insights and information.

[71] Second, the named person and his public counsel can send an unlimited amount of one-way communications to the special advocates at any time throughout the proceedings. This is significant. As discussed above, the public summaries provided on an ongoing basis to the named person will ensure that he or she is sufficiently informed to provide meaningful guidance and information to the special advocates. These summaries should elicit helpful one-way communications from the named person to the special advocates. And these one-way communications may in turn give rise to requests from the special advocates for judicial permission to communicate with the named person in order to obtain needed clarifications or additional information.

[72] Finally, the record does not support the conclusion that the *IRPA* scheme is unconstitutional on the basis that the special advocates must necessarily breach solicitor-client privilege in order to obtain judicial permission to communicate. As Noël J. noted, “[t]he question of assessing solicitor-client [privilege] remains theoretical in the case at hand. The requests to communicate presented did not directly or indirectly reveal such information”: 2010 FC 1242, at para. 178. Moreover, the evolving practices of the Federal Court may substantially lessen the tension between judicial authorization and privilege. For example, the special advocates can minimize the risk of revealing their litigation strategy by seeking to

make submissions to the designated judge in the absence of the ministers' lawyers:  
*Almrei*, 2008 FC 1216, at para. 65.

[73] The issue of how to reconcile the judicial authorization process with solicitor-client privilege should be decided if and when it arises on the facts of a case: *Almrei*, 2008 FC 1216, at para. 41; *Almrei*, 2009 FC 322, 342 F.T.R. 11, at para. 24. It may be that an exception to solicitor-client privilege could be recognized in such circumstances: *Smith v. Jones*, [1999] 1 S.C.R. 455, at para. 53, *per Cory J.*; *Almrei*, 2008 FC 1216, at paras. 60-62. Or it may instead be necessary to recognize that, in cases where judicial authorization cannot be granted without a breach of solicitor-client privilege, the proceedings fail to meet the requirements of s. 7 of the *Charter* and that a remedy should be granted under s. 24(1) of the *Charter*.

*Does the Admission of Hearsay Evidence Render the Scheme Unconstitutional?*

[74] The *IRPA* scheme provides that the usual rules of evidence do not apply to the security certificate proceedings. Rather, any evidence that the judge determines to be "reliable and appropriate" is admissible: s. 83(1)(h), *IRPA*. It is argued that this denies the named person's s. 7 *Charter* rights, since the special advocates will be unable to meaningfully test the evidence.

[75] It is true that some evidence which is admissible under the *IRPA* scheme cannot be tested for reliability and accuracy in the usual manner. For example, the *IRPA* scheme would allow the admission of a foreign intelligence agency's report that

the judge deems “reliable and appropriate”, despite the fact that it is hearsay. The special advocates will not have had the opportunity to cross-examine the foreign sources quoted in the report or the operatives who compiled it.

[76] While s. 83(1)(h) of the *IRPA* may result in the admission of hearsay evidence and deny the special advocates the ability to cross-examine sources, it does not violate s. 7 of the *Charter*. As this Court recognized in *R. v. L. (D.O.)*, [1993] 4 S.C.R. 419, “the rules of evidence have not been constitutionalized into unalterable principles of fundamental justice”: p. 453, *per* L’Heureux-Dubé J. As discussed, s. 7 guarantees a fundamentally fair process. The rule against hearsay evidence and the right to cross-examine witnesses simply provide a means towards such a process, by screening out unreliable evidence: *R. v. Khelawon*, 2006 SCC 57, [2006] 2 S.C.R. 787, at para. 48. The *IRPA* scheme achieves this purpose of excluding unreliable evidence by alternative means. It provides the designated judge with broad discretion to exclude evidence that is not “reliable and appropriate”. This broad discretion allows the judge to exclude not only evidence that he or she finds, after a searching review, to be unreliable, but also evidence whose probative value is outweighed by its prejudicial effect against the named person.

#### Concluding Remarks on the Constitutionality of the *IRPA* Scheme

[77] I have concluded that the impugned provisions of the *IRPA* scheme are constitutional. They do not violate the named person’s right to know and meet the case against him, or the right to have a decision made on the facts and the law.

However, it must be acknowledged that these provisions remain an imperfect substitute for full disclosure in an open court. There may be cases where the nature of the allegations and of the evidence relied upon exacerbate the limitations inherent to the scheme, resulting in an unfair process. In light of this reality, the designated judge has an ongoing responsibility to assess the overall fairness of the process and to grant remedies under s. 24(1) of the *Charter* where appropriate — including, if necessary, a stay of proceedings.

*Are CSIS Human Sources Covered by Privilege and Can They Be Cross-Examined?*

[78] Mr. Harkat's special advocates ask the Court for an order permitting them to interview and cross-examine the CSIS human sources relied upon by the Minister in the case against him. Noël J. denied this order, holding that the identity of the sources and information which tends to reveal their identity is covered by a common law "class" privilege.

[79] The Federal Court of Appeal disagreed. It held that, unlike police informers, CSIS human sources are not protected by common law class privilege. However, it did not deal with whether the human sources could be cross-examined.

[80] I agree with the Federal Court of Appeal that CSIS human sources are not protected by a class privilege. However, this is not to say that they are left entirely unprotected by the security certificate regime. The *IRPA* scheme provides a mechanism to protect their identity, as I will now discuss.

### Does Privilege Attach to CSIS Human Sources?

[81] It is important to note at the outset that the *IRPA* scheme provides protection for the identity of sources and of information that tends to reveal that identity. Indeed, the starting point under the *IRPA* scheme is that all information whose disclosure would be injurious to national security or endanger the safety of a person is protected from disclosure to the named person and to the public: s. 83(1)(d). In most cases, the disclosure of the identity of human sources would both be injurious to national security and endanger the safety of those sources. Consequently, their identity will generally be protected from disclosure under the *IRPA* scheme.

[82] As a limited exception to this general principle of non-disclosure, the *IRPA* scheme provides that special advocates get full disclosure of all the evidence provided by the Minister to the judge: s. 85.4(1). The Minister has no obligation, however, to disclose privileged materials to anyone.

[83] It thus becomes necessary to determine whether the identities of CSIS human sources, and related information, are privileged. But it is important to bear in mind that even if they are not privileged, the judge under the *IRPA* scheme has the duty to prevent disclosure to the public and to the named person of this information if it would be injurious to national security or the safety of the sources. The information will thus generally remain within the confines of the closed circle formed by the designated judge, the special advocates — who, it bears repeating, are security-cleared lawyers — and the Minister's lawyers.

[84] Against this background, I come to the question: Are the identities of CSIS human sources and information that might reveal their identity protected by common law privilege?

[85] It is argued that police informer privilege attaches to CSIS human sources. I agree with the Federal Court of Appeal that it does not. Traditional police work involving informers, on the one hand, and the collection of security intelligence and information, on the other, are two different things. Indeed, Parliament created CSIS in recognition of this emerging distinction: *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326 (“*Charkaoui II*”), at paras. 21-22. Courts developed police informer privilege at a time when the police investigated crimes locally and collected evidence mainly for use in criminal trials. By contrast, the intelligence gathering conducted by CSIS takes place on a global scale and is geared towards prospectively preventing risks: K. Roach, “The eroding distinction between intelligence and evidence in terrorism investigations”, in N. McGarrity, A. Lynch and G. Williams, eds., *Counter-Terrorism and Beyond: The Culture of Law and Justice after 9/11* (2010), 48. Police have an incentive not to promise confidentiality except where truly necessary, because doing so can make it harder to use an informer as a witness. CSIS, on the other hand, is not so constrained. It is concerned primarily with obtaining security intelligence, rather than finding evidence for use in court. While evidence gathered by the police was traditionally used in criminal trials that provide the accused with significant evidentiary safeguards, the intelligence gathered by CSIS may be used to establish criminal conduct in

proceedings that — as is the case here — have relaxed rules of evidence and allow for the admission of hearsay evidence. The differences between traditional policing and modern intelligence gathering preclude automatically applying traditional police informer privilege to CSIS human sources.

[86] I have found no persuasive authority for the proposition that police informer privilege applies to CSIS human sources. In *R. v. Y.(N.)*, 2012 ONCA 745, 113 O.R. (3d) 347, cited as authority by Abella and Cromwell JJ., the issue was whether an informer who had worked successively for CSIS and the RCMP was a state agent for purposes of applying the *Charter*. The court remarked that one distinction between a state agent and a confidential informer is that privilege applies only to the latter (para. 122). The court's reasons can be read as assuming that privilege would attach to a CSIS informer, but that point was not squarely before the court and was not decided.

[87] Nor, in my view, should this Court create a new privilege for CSIS human sources. This Court has stated that “[t]he law recognizes very few ‘class privileges’” and that “[i]t is likely that in future such ‘class’ privileges will be created, if at all, only by legislative action”: *R. v. National Post*, 2010 SCC 16 [2010] 1 S.C.R. 477, at para. 42. The wisdom of this applies to the proposal that privilege be extended to CSIS human sources: *Canada (Attorney General) v. Almalki*, 2011 FCA 199, [2012] 2 F.C.R. 594, at paras. 29-30, *per* Létourneau J.A. If Parliament deems it desirable that CSIS human sources' identities and related information be privileged,

whether to facilitate coordination between police forces and CSIS or to encourage sources to come forward to CSIS (see reasons of Abella and Cromwell JJ.), it can enact the appropriate protections. Finally, the question arises whether judges should have the power to shield the identity of human sources from special advocates on a case-by-case basis where they conclude that public interests in non-disclosure outweigh the benefits of disclosure. This question was not argued by the parties, and I offer no comment on it, other than to note that the *IRPA* scheme already affords broad protection to human sources by precluding the public disclosure of information that would injure national security or endanger a person.

Should the Special Advocates Be Authorized to Interview and Cross-Examine the Human Sources?

[88] The special advocates ask this Court to rule that they may interview and cross-examine the CSIS human sources who have provided information used against Mr. Harkat.<sup>1</sup> I have concluded that the identity of CSIS human sources is not privileged. However, it does not follow from the absence of a privilege that special advocates have an unlimited ability to interview and cross-examine human sources. As discussed above, the designated judge may admit information provided by these sources as hearsay evidence, if he concludes that the evidence is “reliable and appropriate”: s. 83(1)(h), *IRPA*. The Minister has no obligation to produce CSIS

---

<sup>1</sup> The special advocates have already had access to the complete human source files. Although the designated judge found that privilege applied to CSIS human sources, he nevertheless ordered disclosure of unredacted versions of the relevant files to the special advocates as a remedy for breaches by the ministers of their obligations towards Mr. Harkat. See 2009 FC 553 and 2009 FC 1050.

human sources as witnesses, although the failure to do so may weaken the probative value of his evidence.

[89] This said, the special advocates may “exercise, with the judge’s authorization, any other powers that are necessary to protect the interests” of the named person: s. 85.2(c), *IRPA*. The designated judge has the discretion to allow the special advocates to interview and cross-examine human sources in a closed hearing. This discretion should be exercised as a last resort. The record before us establishes that a generalized practice of calling CSIS human sources before a court, even if only in closed hearings, may have a chilling effect on potential sources and hinder CSIS’ ability to recruit new sources. In most cases, disclosure to the special advocates of the human source files and other relevant information regarding the human sources will suffice to protect the interests of the named person.

[90] The case at hand is not one of those rare cases in which it is necessary to give special advocates permission to interview and cross-examine CSIS human sources. The special advocates contend that cross-examination is necessary in order to test the credibility of the human sources, to cross-examine them on Mr. Harkat’s motives for coming to Canada in the mid-1990s, and to undermine the allegation that Mr. Harkat traveled to Afghanistan. In my view, Mr. Harkat and his special advocates have had sufficient opportunity to pursue those objectives, and the designated judge’s weighing of the relevant evidence took into account the fact that it was hearsay. Indeed, the evidence on the record allowed the special advocates to undermine the

credibility of one of the human sources and led Noël J. to rely on information originating from this source only when corroborated: see 2010 FC 1241, [2012] 3 F.C.R. 251, at footnote 1. Moreover, Mr. Harkat testified with respect to his motives for coming to Canada and denied the allegations that he visited Afghanistan. Noël J. made a strong adverse finding of credibility against Mr. Harkat on these issues: it is highly improbable that cross-examination of the human sources could have bolstered his credibility. There is therefore no need for this Court to authorize the exceptional measure of interviewing and cross-examining human sources.

*Did the Designated Judge Err in Refusing to Exclude the Summaries of Intercepted Conversations?*

[91] Mr. Harkat seeks the exclusion of summaries of intercepted conversations that were tendered as evidence by the ministers, pursuant to s. 24(1) of the *Charter*. He argues that CSIS prejudiced his ability to know and meet the case against him by destroying the original operational notes and recordings that were the source materials for the summaries. Noël J. found the summaries to be reliable and concluded that the destruction of the operational materials did not prejudice Mr. Harkat. The Federal Court of Appeal disagreed, finding that the destruction of the materials prejudiced Mr. Harkat's ability to challenge the reliability and accuracy of the summaries. As a remedy, it excluded the summaries of intercepted conversations to which Mr. Harkat was not privy.

Did the Destruction of Source Materials Result in a Breach of Section 7 of the *Charter*?

[92] The original CSIS operational materials were destroyed in accordance with CSIS internal policy OPS-217, which required the systematic destruction of operational materials after operatives had completed their final reports and summaries. In *Charkaoui II*, this Court found that both the *Canadian Security Intelligence Service Act*, R.S.C. 1985, C-23 (“*CSIS Act*”), and the right to procedural fairness of the named person required CSIS “to retain all the information in its possession and to disclose it to the ministers and the designated judge”: para. 62.

[93] As a result of policy OPS-217, the original operational notes and recordings are lost evidence. Where the Minister loses evidence that should have been disclosed, he has a duty to explain what happened to it: *R. v. La*, [1997] 2 S.C.R. 680, at paras. 18-20. Where the Minister is unable to satisfy the judge that the evidence was not destroyed owing to unacceptable negligence, he has failed to meet his disclosure obligations and there has been a breach of s. 7 of the *Charter*: *La*, at para. 20. In the present case, the destruction of operational notes pursuant to policy OPS-217 constitutes unacceptable negligence, within the meaning of *La*. Indeed, no reasonable steps were taken to preserve the evidence: *La*, at para. 21. Quite the contrary. CSIS destroyed the materials in violation of the *CSIS Act*, and, in so doing, compromised “the very function of judicial review”: *Charkaoui II*, at para. 62. Consequently, the ministers failed to meet their disclosure obligations towards Mr. Harkat and breached s. 7 of the *Charter*.

#### What Is the Appropriate Remedy?

[94] The finding that CSIS operational materials were destroyed through unacceptable negligence does not necessarily mean that the summaries of those materials must be excluded from the evidence. The appropriate remedy for the destruction of materials pursuant to policy OPS-217 must be assessed on a case-by-case basis, and must be tailored to address the prejudicial effect on the named person's case: *Charkaoui II*, at para. 46.

[95] The summaries of materials destroyed pursuant to policy OPS-217 should only be excluded under s. 24(1) of the *Charter* if their admission “would result in an unfair trial or would otherwise undermine the integrity of the justice system”: *R. v. Bjelland*, 2009 SCC 38, [2009] 2 S.C.R. 651, at para. 3. “[T]he appropriate focus in most cases of late or insufficient disclosure under s. 24(1) is the remediation of prejudice to the accused” and the “safeguarding of the integrity of the justice system”: *ibid.*, at para. 26. Since the exclusion of evidence impedes the truth-seeking function of trials, it should only be resorted to if lesser remedies are inadequate to achieve those two purposes: *ibid.*, at para. 24.

[96] Thus, the question here is whether the exclusion of the summaries is necessary to remedy the prejudice to Mr. Harkat's ability to know and meet the case against him, or to safeguard the integrity of the justice system. In my view, it is not.

[97] The disclosure of the summaries in an abridged version to Mr. Harkat and in an unredacted form to his special advocates was sufficient to prevent significant prejudice to Mr. Harkat's ability to know and meet the case against him. It is true, as

the Federal Court of Appeal noted, that the destruction of the originals makes it impossible to ascertain with complete certainty whether the summaries contain errors or inaccuracies: para. 133. “An assessment of prejudice is problematic where, as in this case, the relevant information has been irretrievably lost”: *R. v. Bero* (2000), 137 O.A.C. 336 , at para. 49. However, the impact of the loss of evidence on trial fairness must be considered “in the context of the rest of the evidence and the position taken by the defence”: *R. v. J.G.B.* (2001), 139 O.A.C. 341, at para. 38.

[98] The destruction of the original operational materials did not significantly prejudice Mr. Harkat’s ability to know and meet the case against him. As Noël J. noted, reliable summaries of the original materials pertaining to the intercepted conversations were disclosed to Mr. Harkat. Mr. Harkat’s position was to deny the very occurrence of most of those conversations rather than to challenge their specifics. And the content of the summaries is corroborated by the overall narrative of Mr. Harkat’s life which emerged during the proceedings: 2010 FC 1243, at paras. 66-67.

[99] Moreover, I am satisfied that the admission of the summaries does not undermine the integrity of the justice system. While the destruction of CSIS operational materials was a serious breach of the duty to preserve evidence, it was not carried out for the purpose of deliberately defeating the Minister’s obligation to disclose. It must also be recognized that, prior to this Court’s holding in *Charkaoui II*, the existence and scope of CSIS’ legal obligation to preserve operational materials

had not been definitively settled by the courts. It cannot be said that CSIS' application of policy OPS-217 evidenced a systematic disregard for the law. Since the admission of the summaries would neither deny procedural fairness to Mr. Harkat nor undermine the integrity of the justice system, I conclude that Noël J. made no reviewable errors in refusing to exclude the impugned summaries of intercepted conversations.

*Did the Ministers Breach Their Duties of Candour and Utmost Good Faith?*

[100] The special advocates argue that duties of candour and utmost good faith required the ministers to make extensive inquiries of foreign intelligence agencies for information and evidence regarding several alleged terrorists with whom they claim that Mr. Harkat had associated. They contend that the ministers failed to discharge these duties. The courts below found that the ministers made reasonable efforts to obtain information sought by the special advocates.

[101] In *Ruby*, this Court recognized that duties of candour and utmost good faith apply when a party relies upon evidence in *ex parte* proceedings: "The evidence presented must be complete and thorough and no relevant information adverse to the interest of that party may be withheld": *Ruby*, at para. 27. The Federal Court added, in *Almrei (Re)*, 2009 FC 1263, [2011] 1 F.C.R. 163, at para. 500 that: "The duties of utmost good faith and candour imply that the party relying upon the presentation of *ex parte* evidence will conduct a thorough review of the information in its possession

and make representations based on all of the information including that which is unfavourable to their case”.

[102] The duties of candour and utmost good faith require an ongoing effort to update, throughout the proceedings, the information and evidence regarding the named person: see, for example, *Almrei*, 2009 FC 1263, at para. 500. The special advocates argue that, pursuant to these duties, the ministers must send detailed requests to foreign intelligence agencies. In their view, those requests must explain the context of security certificate hearings, the purposes for which the information will be used, and the consequences for the named person if the information is not provided.

[103] The position advocated by the special advocates is tantamount to requiring the ministers to conduct an investigation under the instructions of the special advocates. The ministers have no general obligation to provide disclosure of evidence or information that is beyond their control: *R. v. Chaplin*, [1995] 1 S.C.R. 727, at para. 21; *R. v. Stinchcombe*, [1995] 1 S.C.R. 754, at para. 2. With respect to evidence and information held by foreign intelligence agencies, the ministers’ duty is to make reasonable efforts to obtain updates and provide disclosure. What constitutes reasonable efforts will turn on the facts of each case. In the present appeal, I agree with Noël J. that reasonable efforts were made by the ministers: see 2010 FC 1243, Annex “A”, at paras. 6-7. The ministers sent letters of request to the relevant foreign intelligence agencies. The outcome of those requests may not have been satisfactory

to the special advocates, but this fact alone is not enough to conclude that the efforts made by the ministers were insufficient.

*Were the Proceedings Against Mr. Harkat Fair?*

[104] The special advocates ask this Court to find that, even if the statutory scheme is constitutional in the abstract, Mr. Harkat was not afforded a fair process in the case at hand and should be granted a stay of proceedings. They contend that they were not given sufficient opportunities to test the reliability and accuracy of the summaries of intercepted conversations and the information provided by foreign intelligence agencies, nor to test the credibility of the human sources.

[105] I would not grant a stay of proceedings. As discussed above, Noël J. did not err in admitting the summaries of intercepted conversations or in refusing to allow the cross-examination of human sources. The special advocates also fail to demonstrate any reviewable errors in his conclusions that the foreign intelligence he admitted was reliable and appropriate, or in the probative value that he accorded to that evidence.

[106] A stay of proceedings is a remedy of last resort, to be granted only in the clearest of cases: *R. v. O'Connor*, [1995] 4 S.C.R. 411, at para. 82; *La*, at para. 23; *Charkaoui II*, at para. 76; *R. v. Babos*, 2014 SCC 16, at para. 31. The special advocates have failed to demonstrate that Mr. Harkat's security certificate

proceedings were an unfair process or that state conduct undermined the integrity of the judicial system. Mr. Harkat is not entitled to a stay of proceedings.

*Did the Designated Judge Err in Concluding That the Security Certificate Was Reasonable?*

[107] Having concluded that Mr. Harkat received a fair process, the only remaining issue is whether Noël J. committed any reviewable errors in concluding that the security certificate referred to him by the ministers was reasonable. Mr. Harkat raises a single argument: that the trial judge erred in his weighing of the evidence.

[108] The designated judge's weighing of the factual evidence on the record is entitled to appellate deference and should only be interfered with if he committed a palpable and overriding error: *Housen v. Nikolaisen*, 2002 SCC 33, [2002] 2 S.C.R. 235. Mr. Harkat identifies only one specific instance where the judge, in his view, committed a palpable and overriding error. He contends that Noël J. erred in finding that an individual named Ibn Khattab facilitated terrorist activities, since a judge in another security certificate case found that Ibn Khattab could not be characterized as engaging in or facilitating terrorism: see *Almrei*, 2009 FC 1263. I cannot accept that submission. In the *Almrei* case, the designated judge was careful to qualify his findings on Ibn Khattab as limited to the facts and the record before him. Indeed, he stated that, "[t]he weight of the evidence before me in this case favours a finding that he [i.e. Ibn Khattab] was not a terrorist in his own right or a terrorist patron but I

accept that there are reasonable grounds to believe the contrary”: para. 457 (emphasis added).

[109] Noël J. was entitled to make his own assessment of whether Ibn Khattab was involved in terrorist activities, based on evidence that he found to be reliable and appropriate. I would not interfere with his assessment. Nor do I find any palpable and overriding error in Noël J.’s weighing of the evidence or in his assessment of Mr. Harkat’s credibility, both of which in his view provided reasonable grounds to establish Mr. Harkat’s inadmissibility.

### Conclusion

[110] The *IRPA* scheme does not provide a perfect process. However, it meets the requirements of procedural fairness that are guaranteed by s. 7 of the *Charter*. The discretion granted to designated judges is the crucial ingredient that allows the proceedings to remain fair from beginning to end. Designated judges must ensure that the named person receives sufficient disclosure of the information and evidence to be able to give meaningful instructions to his public counsel and meaningful guidance to his special advocates, must refuse to admit evidence that is unreliable or whose probative value is outweighed by its prejudicial effects, and must take a liberal approach towards authorizing communications by the special advocates. And in cases where the inherent limitations of the *IRPA* scheme create procedural unfairness, designated judges must exercise their discretion under s. 24(1) of the *Charter* to grant an appropriate remedy.

[111] In the present case, Mr. Harkat benefited from a fair process. The designated judge did not err in refusing to exclude summaries of intercepted conversations and to allow the cross-examination of human sources. In addition, he did not commit a palpable or overriding error in concluding that the record provided reasonable grounds to find that Mr. Harkat was inadmissible on security grounds. Consequently, I would allow the appeal in part and dismiss the cross-appeal. Noël J.'s conclusion that the security certificate was reasonable is reinstated.

[112] At the closed hearing, the ministers requested that they be allowed to review these reasons before they are released to Mr. Harkat and to the public. I would not allow this. The information contained within these reasons has already been publicly disclosed in the reasons of the courts below; it poses no risk to national security.

The following are the reasons delivered by

ABELLA AND CROMWELL JJ. —

[113] An individual who comes forward with information about a potential terrorist threat, often risks his or her life in doing so if his or her identity is disclosed. Offering the possibility of anonymity only if a court subsequently agrees to protect the source's identity, requires the source to choose between risk of personal harm if his identity is not protected, or risk of harm to the public if the information is not

disclosed. That is the inevitable result of a case-by-case approach as suggested by the majority. In our view, with respect, this choice is not only an unacceptable one from the point of view of the public's safety, it is unnecessary.

[114] Like Noël J., in our view, CSIS informants who provide national security information based on a promise of confidentiality are entitled to the assurance that the confidentiality will be protected. This can only be guaranteed by a class privilege, as is done in criminal law cases. A case-by-case approach results in a source not knowing the likelihood the promise will be kept until a judge engages in a retrospective assessment as to whether the promise will be kept. This is hardly conducive to encouraging informants to risk their lives by coming forward to offer highly sensitive information in terrorism cases. While we otherwise agree with the reasons of the Chief Justice, therefore, we do not share her view of what protection national security sources are entitled to.

### Analysis

[115] Informer privilege has been judicially recognized for more than two centuries and has a dual purpose: protection of a channel of information and the safety of those supplying it (Stanley A. Schiff, *Evidence in the Litigation Process* (4th ed. 1993), at pp. 1550-56). As Professor Schiff explains:

The rationale of the privilege makes it available in all manner of proceedings, including those before commissions of enquiry and administrative tribunals. *The rationale also makes it available if the*

*informant spoke to a public agency other than the police, so long as the agency has law enforcement authority. . . . By the same token, the privilege is not available if the public official to whom the informer spoke has no law enforcement authority . . . .* [Emphasis added; pp. 1551-52.]

[116] It has therefore been applied in settings other than criminal prosecutions, including commissions of inquiry: *Bisaillon v. Keable*, [1983] 2 S.C.R. 60. Numerous decisions of the Federal Court have applied informer privilege to sources who provided confidential information to a parole board (see *Rice v. National Parole Board* (1985), 16 Admin. L.R. 157 (T.D.), at pp. 167-68; *Wilson v. National Parole Board* (1985), 10 Admin. L.R. 171 (T.D.), at p. 188; *Cadieux v. Director of Mountain Institution*, [1985] 1 F.C. 378 (T.D.), at pp. 397-98). It has also been applied to an informer of a securities regulator: *A. v. Drapeau*, 2012 NBCA 73, 393 N.B.R. (2d) 76.

[117] Wigmore refers to the informer privilege as one relating to

the identity of persons supplying the government with information concerning the commission of crimes. . . .

. . .

. . . the principle is a large and flexible one. It applies wherever the situation is one where without this encouragement the citizens who have special information of a violation of law might be deterred otherwise from voluntarily reporting it to the appropriate official. [Emphasis deleted.]

(John Henry Wigmore, *Evidence in Trials at Common Law* (McNaughton rev. 1961), vol. 8, at pp. 761 and 767-68).

[118] This Court has repeatedly held that unlike Crown privilege or privileges based on Wigmore's four-part test, the police informer privilege does not permit a balancing of the benefits of protecting the privileged information against countervailing benefits: *Bisaillon*, at pp. 93-98. This recognizes that the danger to the safety of the informer and to the intelligence-gathering process is considered to be too great to permit the consideration of countervailing factors: *R. v. Leipert*, [1997] 1 S.C.R. 281, at para. 12; *Named Person v. Vancouver Sun*, [2007] 3 S.C.R. 253, at paras. 19-22. In *Bisaillon*, this Court stated:

This procedure, designed to implement Crown privilege, is pointless in the case of secrecy regarding a police informer. In this case, the law gives the Minister, and the Court after him, no power of weighing or evaluating various aspects of the public interest which are in conflict, since it has already resolved the conflict itself. It has decided once and for all, subject to the law being changed, that information regarding police informers' identity will be, because of its content, a *class of information which it is in the public interest to keep secret*, and that this interest will prevail over the need to ensure the highest possible standard of justice. [Emphasis added; pp. 97-98.]

[119] In *R. v. Basi*, [2009] 3 S.C.R. 389, at para. 44, this Court went so far as to conclude that allowing counsel to participate in an *in camera* hearing involving a police informant was impermissible, even if they undertook not to disclose any privileged information:

No one outside the circle of privilege may access information over which the privilege has been claimed until a judge has determined that the privilege does not exist or that an exception applies.

[120] The privilege for informers in the context of state officials investigating matters of national security is not a “new” privilege, but a well-established one. The Ontario Court of Appeal has recognized a common law CSIS source privilege: *R. v. Y. (N.)*, 2012 ONCA 745, 113 O.R. (3d) 347. This case involved the transfer of Shaikh, an informant, from CSIS to the RCMP. One issue before the court was whether the informant had at some point become a state agent for the purposes of entrapment and abuse of process analyses. The court accepted that Shaikh had informant status while working with CSIS: see paras. 12 and 120. The court’s conclusion that Shaikh was not a state agent was premised in part on the fact that he had not intended to waive the confidentiality protections associated with his informant status: paras. 123-25. The court defined a “confidential informant” as a “voluntary source of information to police or security authorities”: para. 122 (emphasis added).

[121] The common law’s protection of informer privilege is based on the common sense recognition that engaging in a case-by-case balancing of interests would frustrate the rationale of informer privilege by discouraging the cooperation of informants. As the U.S. Supreme Court explained in a related context, leaving disclosure to individual judges would cause national security sources to “close up like a clam”: *Central Intelligence Agency v. Sims*, 471 U.S. 159 (1985), at p. 175.

[122] This Court recognized the breadth of the privilege in *Solicitor General of Canada v. Royal Commission of Inquiry into the Confidentiality of Health Records in*

*Ontario*, [1981] 2 S.C.R. 494. The issue was whether RCMP officers could be compelled to disclose to the Commission the identities of individuals who, based on an assurance of confidentiality, gave information to police officials. The Court concluded that the privilege prevented disclosure. The Court held that the immunity from disclosure is “general in scope”, applying not only in criminal proceedings but also in civil proceedings, before commissions of inquiry and in “forensic investigations” generally (p. 536). Writing for the majority, Martland J. emphasized that the rationale which supports the privilege applies with even more cogency in the national security context:

A large number of the instances in which, in the present case, it was sought to obtain from the police the names of their informants concerned police investigation into potential violence against officers of the state, including heads of state. These investigations were admittedly proper police functions. *The rule of law which protects against the disclosure of informants in the police investigation of crime has even greater justification in relation to the protection of national security against violence and terrorism.* [Emphasis added; p. 537.]

[123] Before CSIS was created as an independent agency, the intelligence function it now carries out was performed by the RCMP Security Service: see Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (the “McDonald Commission”), First Report, *Security and Information* (1979), and Second Report, *Freedom and Security under the Law*, vols. 1 and 2 (1981). The McDonald Commission, which led to the creation of an independent intelligence agency in Canada, was of the view that informer privilege

applied to RCMP officers performing intelligence work: see Second Report, vol. 2, at pp. 1162-63. It explained the importance of preserving informant confidentiality as follows:

Security and intelligence activities cannot be carried out effectively without the use of informants. Informants are the main source of information for security and intelligence agencies. Whether the informants are paid or voluntary they invariably provide the information on the basis that their identity will be kept secret and that every effort will be made to ensure that it remains so. Their reasons for wanting their identity to remain secret are myriad and include fear of physical retaliation, harassment or ostracism. Any uncertainty about the ability of agencies to keep sources confidential will result in a “drying up” of such sources.

(First Report, at p. 42)

[124] The mandate of the RCMP Security Service was set out in a cabinet directive of 1975 as being to “discern, monitor, investigate, deter, prevent and counter’ persons engaging in subversive or other activity inimical to national security”: Parliamentary Research Branch, “The Canadian Security Intelligence Service” (2000), Current Issue Review 84-27E, at p. 4. Those functions are now found in s. 12 of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, which states that “[t]he Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.”

[125] As this Court pointed out in *Charkaoui v. Canada (Citizenship and Immigration)*, [2008] 2 S.C.R. 326 (“*Charkaoui II*”), “the activities of the RCMP and those of CSIS have in some respects been converging”: para. 26. There is no doubt that informer privilege applied to RCMP Security Service informants. While it is true that the functions of CSIS and the RCMP are distinct, the rationale for the informer privilege applies equally to the work of both. The transfer of functions from the RCMP Security Service to CSIS should have no bearing on whether the privilege continues to exist. The investigatory and monitoring services CSIS performs are those previously carried out by the RCMP. There has been a statutory transfer, but not a functional one.

[126] The erection of an artificial boundary between them could lead to absurd results. A source who began supplying information to the police regarding a suspected terrorist threat and then later provided information to CSIS would be entitled to the privilege with respect to the former but not the latter interaction, even if the same assurances of privilege had been given by both agencies. This is not an abstract problem, given the frequent cooperation between the two agencies.

[127] Two recent cases illustrate the way sources are shared in national security investigations: *R. v. Ahmad*, 2009 CanLII 84776 (Ont. S.C.J.), at paras. 31-34; *Y. (N.)*, at para. 120. *Ahmad* involved information obtained by CSIS and shared with the RCMP, which led to criminal prosecutions for terrorism offences. *Y. (N.)* involved the transfer of a human source from CSIS to the RCMP. In *Ahmad*, Dawson J. made the

following observation about the nature of the relationship between CSIS and the RCMP:

. . . situations will arise where some sharing of information must occur if each organization is to fulfill its mandate. For example, where CSIS comes into possession of information of a real threat to national security, or learns of serious criminal activity, it must notify the RCMP. As Mr. Brooks indicated at para. 15 of his affidavit, CSIS will normally be engaged in the investigation of threats to the security of Canada before the police would have sufficient evidence to commence an investigation on their own. He also points out in his evidence that intelligence gathering investigations are very open ended and wide ranging, with the focus on looking for trends and relationships to help predict emerging or future threats. Such investigations are not oriented towards prosecution. It is the function of the police to react to any information provided by CSIS and to determine how best to proceed from a police perspective. [para. 34]

[128] To argue that it is unjust for the ministers to claim privilege over the identity of CSIS human sources while continuing to rely on the information obtained from them, is to forget the significant distinction between whether the privilege exists and whether the information provided by the human source can be used to establish the reasonableness of the certificate. Where the information has been redacted and anonymized so that the identity of the human source cannot be ascertained, there is no reason that it must always be eliminated from consideration by the designated judge. There is an obvious analogy to the well-settled law that permits confidential informant information to be considered, for example, in an information to obtain a search warrant and in a wiretap authorization: *R. v. Debot*, [1989] 2 S.C.R. 1140; *R. v. Garofoli*, [1990] 2 S.C.R. 1421, at p. 1456. In these contexts, the law has developed

some protections, but under certain conditions it nonetheless allows the confidential source material to be considered without the cross-examination of the source.

[129] Noël J. found that “the recruitment of human sources would be harmed if the guarantees of confidentiality given by the Service were not upheld by this Court”: 2009 FC 204, at para. 28. He set out some possible safeguards and lines of inquiry that could help ensure that anonymous source material is sufficiently reliable that it could fairly be considered as part of the review of the reasonableness of the certificate: paras. 64-67. In addition, if a reviewing judge were of the view that consideration of confidential source material would result in a review hearing that does not meet the *Charkaoui II* standard, the judge could exclude that information from consideration.

[130] There may also be limited circumstances in which the special advocates could be granted access to the privileged information, namely where it is necessary so that the validity of the claim of privilege can be tested. In a criminal trial, the trial judge can look at privileged information where doing so is necessary to establish that the privilege is properly claimed. In *Vancouver Sun* and in *Basi*, at para. 57, it was held that in certain circumstances an *amicus curiae* may be considered to be part of the “circle of privilege”.

[131] The special advocates may play a similar role in closed proceedings. While this Court held in *Basi* that it was impermissible for the accused’s counsel to view privileged information based on the need to preserve the integrity of the

solicitor-client relationship, different considerations apply to special advocates. The special advocate is not in a solicitor-client relationship. Furthermore, he or she is subject to heightened security clearance requirements which reduce the risk that disclosure may pose. As a result, if the designated judge believes that submissions by special advocates could assist in determining whether a privilege claim is valid, they may be entitled to view the privileged information. Submissions based on information identifying the human source should be limited to the validity of the privilege claim and not extend to the reliability of the information.

[132] Nor do we think the privilege is abrogated by statute. The Federal Court of Appeal was of the view that when Parliament enacted the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 (“*IRPA*”), it comprehensively legislated the disclosure obligations of the Minister in the security certificate context such that there was no room for importing common law privileges to qualify the disclosure obligations of the Minister. Since ss. 77(2) and 83(1)(c) to (e) of *IRPA* specify that the Minister and judge may not disclose information which is injurious to national security or which puts the safety of any person at risk, recognizing a class privilege would mean that disclosure could be withheld in a case where neither of these two factors was present.

[133] We are unpersuaded that the common law has been ousted by these provisions. In order to abrogate a common law privilege, Parliament must clearly express an intention to do so: see *Canada (Privacy Commissioner) v. Blood Tribe*

*Department of Health*, [2008] 2 S.C.R. 574, at para. 26. *IRPA* makes no reference to informer privilege and, as discussed later in these reasons, does not evince a clear intention to deprive CSIS human sources of its benefit.

[134] *IRPA* also fails to distinguish between what disclosure means in the context of ss. 77(2) and 83(1)(c) to (e) and what it means in the context of disclosing privileged information to the special advocates. Section 77(2) of *IRPA* provides that the Minister must file with the court the information and other evidence on which the security certificate is based. On the other hand, disclosure of information subject to informer privilege raises different considerations. This information will generally not have been provided to the judge under s. 77(2) and so will not form part of the judge's decision on the reasonableness of the issuance of the security certificate. The only provision of *IRPA* which would govern such a scenario is s. 85.2, which sets out the powers of a special advocate, and, in particular, s. 85.2(c), which states that a special advocate may "exercise, with the judge's authorization, any other powers that are necessary to protect the interests of the permanent resident or foreign national". The same analysis applies with respect to ss. 37 and 38 of the *Canada Evidence Act*, R.S.C. 1985, c. C-5. This Court held in *Basi* that where a claim of informer privilege falls under s. 37 of the *Canada Evidence Act*, the usual public interest balancing exercise under s. 37(5) is displaced by the common law privilege: paras. 23-24. Additional protection is therefore provided for national security secrets but without abrogating the underlying common law privileges.

[135] The final question relates to whether an exception to the privilege should apply in the security certificate context. Noël J. was of the view that there was a “need to know” exception, analogous to the “innocence at stake” exception to the police informer privilege. This exception means that the privilege can be set aside in cases where maintaining it would undermine the accused’s ability to raise a reasonable doubt. The “need to know” exception would similarly be engaged when abrogating the privilege is necessary to prevent a serious breach of procedural fairness that would impugn the administration of justice. On the facts before him, Noël J. held that the requirements of the “need to know” exception had not been met and therefore denied the special advocates’ request.

[136] In our view, the “need to know exception” outlined by Noël J. is overly broad: 2009 FC 204, at para. 46. We agree with the ministers that this exception is broader than the “innocence at stake” exception because the latter applies only where there is a risk of an unjust outcome, whereas the “need to know” exception applies where there is an unjust procedure. It also appears to overlook the considerable procedural flexibility that is available to the reviewing judge and the particular role of the special advocate.

[137] But given the intensity of the interests at stake in the security certificate context, we acknowledge that it would be appropriate to recognize a limited exception specifically crafted for the security certificate process which would address only disclosure to the special advocate, not to the subject of the proceedings. Identity

should be disclosed only if the reviewing judge is satisfied that other measures, including withdrawing the substance of the informant's evidence from consideration in support of the certificate, are not sufficient to ensure a just outcome. Noël J. ordered generous disclosure of material to the special advocates concerning the credibility of informers and the information they supplied. He allowed cross-examination of CSIS witnesses on the value, reliability and usefulness of informer information. In some circumstances, he relied on informer information only where it had been corroborated. If these measures are not considered adequate, the reviewing judge also has discretion under s. 83(1)(h) of *IRPA* to refuse to rely on evidence that he or she does not consider to be reliable and appropriate. Only if resort to these measures would not ensure a just outcome should identity be disclosed.

[138] Even when disclosure of identity is ordered, there should be no cross-examination of the source by the special advocate. Requiring a human source to testify will have a profound chilling effect on the willingness of other sources to come forward, and will undoubtedly damage the relationship between CSIS and the source compelled to testify. CSIS operatives must be able to provide confident assurances to their sources that their identities will not be revealed, not vague assurances hedged with qualifications. Moreover, the human sources themselves, who are not subject to the necessary security clearance, may learn sensitive material in the closed proceedings which CSIS will then be unable to control.

[139] We would therefore allow the ministers' appeal on the informant privilege issue and restore Noël J.'s disposition of this issue.

## APPENDIX

*Immigration and Refugee Protection Act, S.C. 2001, c. 27*

**33.** The facts that constitute inadmissibility under sections 34 to 37 include facts arising from omissions and, unless otherwise provided, include facts for which there are reasonable grounds to believe that they have occurred, are occurring or may occur.

**34.** (1) A permanent resident or a foreign national is inadmissible on security grounds for

(a) engaging in an act of espionage that is against Canada or that is contrary to Canada's interests;

(b) engaging in or instigating the subversion by force of any government;

(b.1) engaging in an act of subversion against a democratic government, institution or process as they are understood in Canada;

(c) engaging in terrorism;

(d) being a danger to the security of Canada;

(e) engaging in acts of violence that would or might endanger the lives or safety of persons in Canada; or

(f) being a member of an organization that there are reasonable grounds to believe engages, has engaged or will engage in acts referred to in paragraph (a), (b), (b.1) or (c).

**77.** (1) The Minister and the Minister of Citizenship and Immigration shall sign a certificate stating that a permanent resident or foreign national is inadmissible on grounds of security, violating human or international rights, serious criminality or organized criminality, and shall refer the certificate to the Federal Court.

(2) When the certificate is referred, the Minister shall file with the Court the information and other evidence on which the certificate is based, and a summary of

information and other evidence that enables the person who is named in the certificate to be reasonably informed of the case made by the Minister but that does not include anything that, in the Minister's opinion, would be injurious to national security or endanger the safety of any person if disclosed.

(3) Once the certificate is referred, no proceeding under this Act respecting the person who is named in the certificate — other than proceedings relating to sections 82 to 82.3, 112 and 115 — may be commenced or continued until the judge determines whether the certificate is reasonable.

**78.** The judge shall determine whether the certificate is reasonable and shall quash the certificate if he or she determines that it is not.

**80.** A certificate that is determined to be reasonable is conclusive proof that the person named in it is inadmissible and is a removal order that is in force without it being necessary to hold or continue an examination or admissibility hearing.

**81.** The Minister and the Minister of Citizenship and Immigration may issue a warrant for the arrest and detention of a person who is named in a certificate if they have reasonable grounds to believe that the person is a danger to national security or to the safety of any person or is unlikely to appear at a proceeding or for removal.

**83.** (1) The following provisions apply to proceedings under any of sections 78 and 82 to 82.2:

(a) the judge shall proceed as informally and expeditiously as the circumstances and considerations of fairness and natural justice permit;

(b) the judge shall appoint a person from the list referred to in subsection 85(1) to act as a special advocate in the proceeding after hearing representations from the permanent resident or foreign national and the Minister and after giving particular consideration and weight to the preferences of the permanent resident or foreign national;

(c) at any time during a proceeding, the judge may, on the judge's own motion — and shall, on each request of the Minister — hear information or other evidence in the absence of the public and of the permanent resident or foreign national and their counsel if, in the judge's opinion, its disclosure could be injurious to national security or endanger the safety of any person;

(d) the judge shall ensure the confidentiality of information and other evidence provided by the Minister if, in the judge's opinion, its disclosure would be injurious to national security or endanger the safety of any person;

(e) throughout the proceeding, the judge shall ensure that the permanent resident or foreign national is provided with a summary of information and other evidence

that enables them to be reasonably informed of the case made by the Minister in the proceeding but that does not include anything that, in the judge's opinion, would be injurious to national security or endanger the safety of any person if disclosed;

(f) the judge shall ensure the confidentiality of all information or other evidence that is withdrawn by the Minister;

(g) the judge shall provide the permanent resident or foreign national and the Minister with an opportunity to be heard;

(h) the judge may receive into evidence anything that, in the judge's opinion, is reliable and appropriate, even if it is inadmissible in a court of law, and may base a decision on that evidence;

(i) the judge may base a decision on information or other evidence even if a summary of that information or other evidence is not provided to the permanent resident or foreign national; and

(j) the judge shall not base a decision on information or other evidence provided by the Minister, and shall return it to the Minister, if the judge determines that it is not relevant or if the Minister withdraws it.

(1.1) For the purposes of paragraph (1)(h), reliable and appropriate evidence does not include information that is believed on reasonable grounds to have been obtained as a result of the use of torture within the meaning of section 269.1 of the *Criminal Code*, or cruel, inhuman or degrading treatment or punishment within the meaning of the Convention Against Torture.

...

**85.1** (1) A special advocate's role is to protect the interests of the permanent resident or foreign national in a proceeding under any of sections 78 and 82 to 82.2 when information or other evidence is heard in the absence of the public and of the permanent resident or foreign national and their counsel.

(2) A special advocate may challenge

(a) the Minister's claim that the disclosure of information or other evidence would be injurious to national security or endanger the safety of any person; and

(b) the relevance, reliability and sufficiency of information or other evidence that is provided by the Minister and is not disclosed to the permanent resident or foreign national and their counsel, and the weight to be given to it.

(3) For greater certainty, the special advocate is not a party to the proceeding and the relationship between the special advocate and the permanent resident or foreign national is not that of solicitor and client.

(4) However, a communication between the permanent resident or foreign national or their counsel and the special advocate that would be subject to solicitor-

client privilege if the relationship were one of solicitor and client is deemed to be subject to solicitor-client privilege. For greater certainty, in respect of that communication, the special advocate is not a compellable witness in any proceeding.

**85.2** A special advocate may

(a) make oral and written submissions with respect to the information and other evidence that is provided by the Minister and is not disclosed to the permanent resident or foreign national and their counsel;

(b) participate in, and cross-examine witnesses who testify during, any part of the proceeding that is held in the absence of the public and of the permanent resident or foreign national and their counsel; and

(c) exercise, with the judge's authorization, any other powers that are necessary to protect the interests of the permanent resident or foreign national.

**85.4** (1) The Minister shall, within a period set by the judge, provide the special advocate with a copy of all information and other evidence that is provided to the judge but that is not disclosed to the permanent resident or foreign national and their counsel.

(2) After that information or other evidence is received by the special advocate, the special advocate may, during the remainder of the proceeding, communicate with another person about the proceeding only with the judge's authorization and subject to any conditions that the judge considers appropriate.

(3) If the special advocate is authorized to communicate with a person, the judge may prohibit that person from communicating with anyone else about the proceeding during the remainder of the proceeding or may impose conditions with respect to such a communication during that period.

**85.5** With the exception of communications authorized by a judge, no person shall

(a) disclose information or other evidence that is disclosed to them under section 85.4 and that is treated as confidential by the judge presiding at the proceeding; or

(b) communicate with another person about the content of any part of a proceeding under any of sections 78 and 82 to 82.2 that is heard in the absence of the public and of the permanent resident or foreign national and their counsel.

*Canada Evidence Act*, R.S.C. 1985, c. C-5, as am. by S.C. 2013, c.9, s.20

**38.06** (1) Unless the judge concludes that the disclosure of the information or facts referred to in subsection 38.02(1) would be injurious to international relations or

national defence or national security, the judge may, by order, authorize the disclosure of the information or facts.

(2) If the judge concludes that the disclosure of the information or facts would be injurious to international relations or national defence or national security but that the public interest in disclosure outweighs in importance the public interest in non-disclosure, the judge may by order, after considering both the public interest in disclosure and the form of and conditions to disclosure that are most likely to limit any injury to international relations or national defence or national security resulting from disclosure, authorize the disclosure, subject to any conditions that the judge considers appropriate, of all or part of the information or facts, a summary of the information or a written admission of facts relating to the information.

...

*Appeal allowed in part, ABELLA and CROMWELL JJ. dissenting in part.*

*Cross-appeal dismissed.*

*Solicitor for the appellants/respondents on cross-appeal: Attorney General of Canada, Toronto and Ottawa.*

*Solicitors for the respondent/appellant on cross-appeal: Webber Schroeder Goldstein Abergel, Ottawa; Bayne, Sellar, Boxall, Ottawa.*

*Solicitor for the intervener the Attorney General of Ontario: Attorney General of Ontario, Toronto.*

*Solicitors for the intervener the British Columbia Civil Liberties Association: Ruby Shiller Chan Hasan, Toronto.*

*Solicitors for the intervener the Canadian Council of Criminal Defence Lawyers: John Norris, Toronto; Poupart, Dadour, Touma & Associés, Montréal.*

*Solicitors for the intervener the Canadian Civil Liberties Association: Kapoor Barristers, Toronto.*

*Solicitors for the intervener the Canadian Bar Association: Waldman & Associates, Toronto; Edelman & Co., Vancouver.*

*Solicitors for the intervener the Canadian Association of Refugee Lawyers: Sack Goldblatt Mitchell, Toronto.*

*Solicitors for the interveners the Canadian Council for Refugees and the International Civil Liberties Monitoring Group: Jackman Nazami & Associates, Toronto; Queen's University, Kingston; Refugee Law Office, Toronto.*

*Solicitors for the intervener the Canadian Council on American-Islamic Relations (now known as National Council of Canadian Muslims): Office Khalid Elgazzar, Barrister, Ottawa; Osgoode Law School of York University, Toronto.*

*Solicitors for the intervener Amnesty International: Community Legal Services-Ottawa Centre, Ottawa; Amnesty International Canada, Ottawa.*

*Solicitors for the intervener the Criminal Lawyers' Association (Ontario): Breese Davies Law, Toronto; Di Luca Copeland, Toronto.*

*Solicitors for the Special Advocates: Cavalluzzo Shilton McIntyre Cornish, Toronto; Copeland, Duncan, Toronto.*