The Problem of "Relevance": Intelligence to Evidence Lessons from UK Terrorism Prosecutions

LEAH WEST *

ABSTRACT

As of November 2017, 60 known foreign terrorist fighters have been permitted to return and live in Canada without criminal consequence. The reason for this, according to the Minister of Public Safety, is the problem of using information collected for intelligence purposes as evidence in criminal proceedings. Often referred to as the "intelligence to evidence" (I2E) dilemma, this challenge has plagued Canada's terrorism prosecutions since the Air India bombing in 1985. Yet, not all countries struggle to bring terrorists to justice. Canada's prosecution statistics pale in comparison to the United Kingdom.

In a democracy committed to upholding the rule of law and respecting human rights, prosecuting terrorists is the strongest and most transparent deterrent to this threat. This article argues that as the threat of terrorism grows both domestically and abroad, Canada must learn from the UK's experience and reform the rules of evidence to ensure that criminal charges are pursued. This article will outline and compare the relevant Canadian and UK rules of evidence and assess their practical implications for national security prosecutions in light of primary research conducted in London in the fall of 2017. It concludes with a series of legislative and organizational reforms to improve the efficiency of Canadian terrorism trials.

* Leah West, MA, JD, is the Anti-Terrorism Research Fellow at the University of Ottawa where she is completing her LLM. She is also counsel with the National Security Litigation and Advisory Group of the Department of Justice. Leah's views are her own and do not reflect the opinion of the Department of Justice.

Keywords: Terrorist; intelligence; evidence; relevance; disclosure; terrorism trial; counter-terrorism; foreign fighter; criminal prosecution; national security

I. INTRODUCTION

As of November 2017, approximately 60 known foreign terrorist fighters have been permitted to return and live in Canada without criminal consequences.[1] Unsurprisingly, political opposition has called on Prime Minister Trudeau's Liberal Government to account for this number, suggesting that the interests of national security require foreign fighters to be targeted and killed before they return home and put Canadians at risk.[2]

In response, the Minister of Public Safety, Ralph Goodale explained that Canada prefers to lay charges rather than target citizens on enemy soil.[3] "When evidence is available charges are laid,"[4] said the Minister in the House of Commons, and "[w]hen prosecutions are possible"[5] he continued, "they are prosecuted to the fullest extent of the law."[6] Yet, between 2001 and 2015 Canada conducted a mere 21 terrorism prosecutions, with only 17 more scheduled to move through the courts in 2016-2017.[7] The

---

1 *House of Commons Debates*, 42nd Parl, 1st Sess, No 234 (20 November 2017) at 15314 (Hon Ralph Goodale) [*Hansard*] ("the director of CSIS indicated before a parliamentary committee some months ago, the number of returnees known to the Government of Canada is in the order of 60, and they are under very careful investigation"); Evan Dyer, "'Canada Does Not Engage in Death Squads,' While Allies Actively Hunt Down Their Own Foreign Fighters," *CBC News* (17 November 2017), online: <http://www.cbc.ca/news/politics/isis-fighters-returning-target-jihadis-1.4404021>.

2 Tonda MacCharles, "Conservatives Slam Trudeau as Soft on Terror as Push for Security Changes Begins," *Toronto Star,* (20 November 2017), online: <https://www.thestar.com/news/canada/2017/11/20/conservatives-slam-trudeau-as-soft-on-terror-as-push-for-security-changes-begins.html>.

3 Evan Dyer, "Does the Law Prevent Canada from Killing Its 'Terrorist Travellers'?" *CBC News* (4 December 2017), online: <http://www.cbc.ca/news/politics/killing-canadian-jihadis-death-squads-1.4429137>.

4 *Hansard*, *supra* note 1 at 15314 (Hon Ralph Goodale).

5 *Ibid.*

6 *Ibid.*

7 Public Prosecution Service of Canada (PPSC), "Report on Plans and Priorities 2016–17," online: <http://www.ppsc-sppc.gc.ca/eng/pub/rpp/2016_2017/index.html#sec

problem, explained Minister Goodale, is one "bedeviling countries around the world in terms of how you actually move from intelligence to evidence and make a case stick."[8]

The intelligence to evidence (I2E) problem has plagued Canada's terrorism prosecutions since the Air India bombing in 1985.[9] However, not all countries struggle to bring terrorist to justice. Canada's prosecution statistics pale in comparison to the United Kingdom, who between 2015 and 2016 prosecuted 79 people for terrorism related offences,[10] and in 2017 arrested 400 more.[11] While there is no doubt that the daily threat of terrorism is greater in the UK,[12] Craig Forcese and Kent Roach argue that

---

tion_2_2>; Public Prosecution Service of Canada, "Transition Book" (February 2017), online: <http://www.ppsc-sppc.gc.ca/eng/tra/tr/08.html>; Craig Forcese & Kent Roach, *False Security: The Radicalization of Canadian Anti-Terrorism* (Toronto: Irwin Law, 2015) at 317–322 [*False Security*].

8 Rachel Gilmore, "Canada Struggling to Prosecute Returned ISIS Fighters," *ipolitics* (26 November 2017), online: <https://ipolitics.ca/2017/11/26/canada-struggling-prosecute-returned-daesh-fighters/>.

9 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence*, *Vol 4* (Ottawa: Public Works and Government Services Canada, 2010) at 12 [*Air India Vol 4*]; Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism*, (Toronto: Cambridge University Press, 2011) at 373.

10 "The Counter-Terrorism Division of the Crown Prosecution Service (CPS) – Cases Concluded in 2015" (19 July 2016), online: <https://www.cps.gov.uk/publications/prosecution/ctd_2015.html:prosecutions that concluded in 2015>; refers to prosecutions concluded in 2015; "The Counter-Terrorism Division of the Crown Prosecution Service (CPS) – Cases Concluded in 2016" (10 February 2017), online: <https://www.cps.gov.uk/publications/prosecution/ctd_2016.html>.

11 UK, Home Office, "Operation of Police Powers Under the Terrorism Act 2000, Quarterly Update to September 2017" (London, UK: Home Office, 2017) at 4 (400 persons were arrested in the year ending 30 September 2017).

12 Vikram Dodd, *The Guardian*, "UK Facing Most Severe Terror Threat Ever, Warns MI5 Chief" (17 October 2017); MI5, "Threat Levels" (December 2017), online: <https://www.mi5.gov.uk/threat-levels> (threat level assessed as severe, meaning an attack is highly likely as of 6 December 2012); Craig Forcese, "Streamlined Anti-terror Investigations: Quick Notes on the UK Experience" (17 November 2017), *National Security Law Blog* (blog), online: <http://craigforcese.squarespace.com/national-security-law-blog/2016/11/17/streamlined-anti-terror-investigations-quick-notes-on-the-uk.html>.

per capita Canada falls behind all of its closest allies when it comes to putting terrorists on trial.[13]

Terrorism is the most significant threat to Canadian national security today.[14] Even if the targeted killing of Canadian foreign fighters directly participating in an armed conflict is legal, as a nation committed to upholding the rule of law and respecting human rights prosecuting terrorists is the strongest and most transparent deterrent Canada has to counter this threat.[15] As the threat of terrorism grows both domestically and abroad, Canada must learn from the UK's experience and reform the rules of evidence to ensure that criminal charges are pursued.

This article will outline and compare the relevant Canadian and UK rules of evidence and assess their practical implications for national security prosecutions in light of primary research conducted in London in the fall of 2017. This comparison will proceed in five parts. First, Part II will review the literature on this topic and describe the research methodology employed by the author. Part III follows with a brief outline of the history of the intelligence to evidence problem in Canada. Part IV will then examine the rules of disclosure in the UK as compared to Canada's common law standard established in *R v Stinchcombe*.[16] This section will also demonstrate how the UK' *Criminal Procedure and Investigations Act 1996* (*CPIA*) empowers

---

13 *False Security, supra* note 7 at 278, 290 (between 2001 and 2014 Canada charged 45 people for terrorism offences; the UK charged 721).

14 Canada, Public Safety Canada, *2014 Public Report on the Terrorist Threat to Canada*, (Ottawa: Public Safety Canada, 2014) at 2. Terrorism is not defined in Canadian law; however, terrorist activity is defined in s 83.01 of the *Criminal Code*, RSC 1985 c C-46. Activities include an open list of acts, most physically violent, that are committed in whole or in part "for a political, religious or ideological purpose" and "with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act" in or out of Canada. Such acts must intentionally (a) cause death or serious bodily harm to a person by the use of violence; (b) endanger a person's life; (c) cause a serious risk to the health or safety of the public; (d) cause substantial property damage; or (e) cause serious interference or serious disruption of an essential service, facility, or system. It also includes being an accessory, conspiracy, counselling and inciting, or the attempt or threat to commit any such act or omission.

15 Craig Forcese & Leah Sherriff, "Killing Citizens: Core Legal Dilemmas in the Targeted Killing of Canadian Foreign Terrorist Fighters" (2016) 57 Cdn YB Intl Law 134; *False Security, supra* note 7 at 274.

16 *R v Stinchcombe*, [1991] 3 SCR 326, 1991 CanLII 45 [*Stinchcombe*];

Crown Prosecutors to act strategically when laying charges and conducting prosecutions to limit the need to rely on and disclose national security material.[17] Part V will establish that the *CPIA* creates little need to rely on the UK's Public Interest Immunity (PII) scheme to prevent the disclosure of national security material; however, when it is necessary, the PII process is more efficient and ensures greater procedural fairness than proceedings conducted under s. 38 of the *Canada Evidence Act* (*CEA*).[18]

Leveraging the lessons learned from the UK, Part VI concludes with an analysis of the *CPIA* in light of the *Canadian Charter of Rights and Freedoms* (*Charter*).[19] Although the principles of fundamental justice protected by s. 7 of the *Charter* would prohibit the wholesale adoption of the UK regime, four legislative and organizational reforms inspired by the *CPIA* are recommended to improve the efficiency of Canadian terrorism trials. These recommendations attempt to respect both the preoccupations of the Canadian Security Intelligence Service (CSIS), and the necessary balance between an accused's right to disclosure and the public interest in prosecuting terrorism.

II. Literature and Methodology

A. Literature

Since 2001, much has been written in Canada and the UK regarding the assertion of national security privilege and the use of secret evidence in criminal and immigration proceedings, and the corresponding impact on the protection of human rights.[20] Canada's struggle to bring charges and

---

17 *Criminal Procedure and Investigations Act 1996*, (1996) UK c 25 [CPIA].

18 *Canada Evidence Act*, RSC 1985, c C-5 [CEA].

19 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

20 Peter Rosenthal, "Disclosure to the Defence After September 11: Sections 37 and 38 of the Canada Evidence Act" (2004) 48 Crim LQ 186; Kathy Grant, "The Unjust Impact of Canada's Anti-Terrorism Act on an Accused's Right to Full Answer and Defence" (2003) 16 Windsor Rev Legal Soc Issues 137; Stephen Townley, "The Use and Misuse of Secret Evidence in Immigration Cases: A Comparative Study of the United States, Canada, and the United Kingdom" (2007) 32 Yale J Intl L 219; Matthew R Hall, "Procedural Due Process Meets National Security: The Problem of Classified Evidence in Immigration Proceedings" (2002) 35 Cornell Intl LJ 515; Jasmina Kalajdzic, "Litigating State Secrets: A Comparative Study of National Security Privilege in Canadian, US and English Civil Cases" (2010) 41:2 Ottawa L Rev 289; Craig Forcese

secure convictions against those suspected of terrorism has also been well documented in the report of the Air India Commission, and in the subsequent publications of Kent Roach and Craig Forcese.[21] Both scholars have repeatedly called for the implementation of the Commission's recommendations, many of which involve reform to Canada's disclosure regime.[22]

Some of the reforms suggested by the Air India Commission however, focus on improving cooperation between Canada's national security agencies, which would more closely reflect the relationship between the UK's MI5 and British law enforcement.[23] The increased capacity for information sharing and joint investigations between these agencies since the attacks on 7/7 has been thoroughly documented by Dr. Frank Foley at King's College London and others.[24] Most recently, David Anderson, the

---

& 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" (2007), online: <https://ssrn.com/abstract=1623509>; Sudha Setty, "Comparative Perspective on Specialized Trials for Terrorism" (2010) 63:1 Me L Rev 131; Daphne Barak-Erez & Matthew C Waxman, "Secret Evidence and the Due Process of Terrorist Detentions" (2009) 48:1 Colum J Transnat'l L 3; Cian C Murphy, "Counter-Terrorism and the Culture of Legality: The Case of Special Advocates" (2013) 24:1 King's LJ 19; Didier Bigo et al, "National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges" in CEPS Paper in Liberty and Security in Europe No 78 (2015); Jeffrey Davis, "Uncloaking Secrecy: International Human Rights Law in Terrorism Cases" (2016) 38:1 Hum Rts Q 58.

21 *Air India Vol 4*, *supra* note 9; Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Final Report, Vol 1* (2010); Kent Roach, "Be Careful What You Wish For? Terrorism Prosecutions in Post-9/11 Canada" (2014) 40 Queen's LJ 99; Kent Roach, "'Constitutional Chicken': National Security Confidentiality and Terrorism Prosecutions after R v Ahmed" (2011) 54:2 SCLR 357; *False Security*, *supra* note 7, ch 9.

22 *Air India Vol 4*, *supra* note 9 at 305–322 (Roach outlines what he refers to as "Back-End Strategies to Reconcile the Demands of Disclosure and Secrecy").

23 *Ibid* at 297–304 (Roach outlines what he refers to as "Front-End Strategies to Make Intelligence Useable in Terrorism Prosecutions").

24 For criticism of Canadian inter-agency cooperation from a UK perspective, see Philip Wright, "Symbiosis or Vassalage? National Security Investigations and the Impediments to Success" in Craig Forcese & François Crépeau, eds, *Terrorism, Law and Democracy: 10 Years after 9/11* (Montreal: Canadian Institute for the Administration of Justice, 2012); Frank Foley, *Countering Terrorism in Britain and France: Institutions, Norms and the Shadow of the Past* (Cambridge: Cambridge University Press, 2013); Frank Foley, "Why Inter-Agency Operations Break Down: US Counterterrorism in Comparative Perspective"

former Independent Reviewer of UK Terrorism Legislation released his assessment of the MI5 and police internal reviews into the 2017 attacks in London and Manchester, providing additional insight into the operational capacities, priorities, and challenges of these organizations.[25]

Since 2016, Forcese has published several pieces comparing the organizational cultural and operational approach to terrorism investigations in the UK and Canada.[26] In the article, "Staying Left of Bang," Forcese draws on lessons learned from the UK and asks skeptically whether Canadian rules of evidence are really to "blame" for the arm's length relationship between the RCMP and CSIS.[27] In his analysis, Forcese identifies that MI5 and law enforcement conduct joint terrorism investigations and, when doing so, MI5 carries out its collection to evidential standards (meaning information is collected in a way that it can be used in court.) As describe bellow, this is not the current practice in Canada as the Canadian disclosure regime strongly disincentives joint investigations.

Forcese's article also sounds the alarm first rung by Joe Fogarty, the former security intelligence liaison between Canada and the UK. Testifying before the Senate, Fogarty warned that Canada has "been remarkably lucky, as a country, that you have not faced fast-moving, sophisticated opponents since 2001 because you could have been living in tragedy here."[28]

(2016) 1:2 European J Intl Security 150; Frank Foley, "The Expansion of Intelligence Agency Mandates: British Counter-Terrorism in Comparative Perspective" (2009) 35:4 Rev Intl Studies 983; Frank Foley, "Reforming Counterterrorism: Institutions and Organizational Routines in Britain and France" (2009) 18:3 Security Studies 435. For more on UK reforms, see Peter Clarke, "Learning From Experience" (The Colin Cramphorn Memorial Lecture 2007 delivered at the Policy Exchange 24 April 2007) (London, UK: Policy Exchange, 2007); Antony Field "Tracking Terrorist Networks: Problems of Intelligence Sharing Within the UK Intelligence Community" (2009) 35 Rev Intl Studies 997; Peter Taylor, "How Britain Has Been Kept Safe for a Decade," *BBC News* (17 July 2016), online: <http://www.bbc.com/news/magazine-36803542>.

25 David Anderson, *Attack in London and Manchester March–June 2017* (December 2017), online: <https://www.gov.uk/government/publications/attacks-in-london-and-manchester-between-march-and-june-2017>.

26 Craig Forcese, "Staying Left of Bang: Reforming Canada's Approach to Anti-Terrorism Investigations" (2017) University of Ottawa Working Paper 2017-23 at 2.

27 *Ibid* at 16–17.

28 Evidence, Standing Senate Committee on National Security and Defence, 41st Parl, 2nd Sess (2 April 2015) (Joe Fogarty) [Evidence of Joe Fogarty].

Mr. Fogarty testified that when serving in Ottawa he advised that the key difference between the operations of the UK and Canada was that CSIS and the RCMP lacked the institutional framework to "share information extensively and also protect themselves from the disclosure" in criminal proceedings.[29] It was his opinion that without the introduction of legislation like the *CPIA*, Canada "could not be as effective in criminal justice terms as it should be."[30]

To date, little has been published in the public domain that validates the claims made by Mr. Fogarty.[31] Thus, this author sought to confirm the importance of the *CPIA* to the working relationship between police and intelligence officers investigating terrorism, and how this facilitates the use of intelligence as evidence by prosecutors in the UK.

B. Methodology

This article undertakes a comparative analyses of the rules of evidence in the UK and Canada, specifically the regimes governing the disclosure of evidence in criminal proceedings, and the applicable privileges available to protect information where the law requires its disclosure but the interests of national security necessitate its protection.

This article does not engage in an assessment of how or why the rules of evidence have evolved with the growth of international terrorism. Rather, the comparison focuses narrowly on the mechanical effect these regimes have had on the conduct of criminal prosecutions for terrorist related activity since 1985 in Canada and 1996 in the UK. The aim of this comparison is to identify differences in the UK regime that increase the efficiency and effectiveness of terrorism prosecutions in that country.

The UK provides an appropriate comparison because, like Canada, it is a common law jurisdiction. As such, the laws of evidence in both jurisdictions are based on the judge and jury model of adjudication, whereby the judge decides questions of law and the jury is responsible for

---

29 *Ibid.*

30 *Ibid.*

31 One exception is a brief article by Susan Hemming of CPS that explains the role of the prosecutor in applying the CPIA, but the article focuses predominantly on the implications of counter-terrorism legislation introduced post 2000. Little is made of the importance of the disclosure test: "The Practical Application of Counter-Terrorism Legislation in England and Wales: A Prosecutor's Perspective" (2010) 86:4 Intl Affairs 955.

questions of fact.[32] The comparison is also relevant because both states have a Westminster-based parliamentary system of government. While the courts in both jurisdictions show deference to the executive branch of government in the realm of national security, this deference is limited by the application of human rights law; in particular, the right to due process and fair trial under article 6 of the *European Convention on Human Rights*,[33] and s. 7 of the *Canadian Charter of Rights and Freedoms*.[34]

The author's research question could not be answered by solely reviewing secondary literature or the relevant legislation, regulations and case law of these jurisdictions. To understand the practical applications of the CPIA in terrorism investigations and prosecutions, and its impact on inter-agency cooperation in the UK, interviews with those who apply and challenge the law was necessary. Interviews with Crown Prosecutors were also required to fully ascertain their role in bringing charges and successfully

---

[32] Howard L Krongold, "A Comparative Perspective on the Exclusion of Relevant Evidence: Common Law and Civil Law Jurisdictions" (2003) 12 Dal LJ 97 at 101. The judge is also responsible for giving jury instructions on how to apply the law, and the judge is responsible for determining what evidence may be admitted and warn the jury about the weight to be given certain evidence. Where the admissibility of evidence is challenged, the judge will consider it in the absence of the jury.

[33] *Convention for the Protection of Human Rights and Fundamental Freedoms* (4 November 1950), 213 UNTS 221, ETS 5 (entered into force 3 September 1950) [*European Convention on Human Rights*].

[34] Aileen Kavanagh, *Constitutional Review under the UK Human Rights Act* (Cambridge: Cambridge University Press, 2009) at 163; Helen Fenwick, Gavin Phillipson & Roger Masterman, "The Human Rights Act in Contemporary Context" in H Fenwick, G Phillipson & R Masterman, eds, *Judicial Reasoning Under the UK Human Rights Act* (Cambridge: Cambridge University Press, 2007) at 2 argues that, while similar, the UK's human rights legislation is not as strong as Canada's); Kent Roach, "Section 7 of the Charter in National Security Cases" (2012) 42 Ottawa L Rev 337. For foundational case law on the interpretation of section 7, see *Re: BC Motor Vehicle Act*, [1985] 2 SCR 486, 1985 CanLII 81; *Canadian Foundation for Children, Youth and the Law v Canada (AG)*, 2004 SCC 4, [2004] 1 SCR 76; *Suresh v Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1, [2002] 1 SCR 3; *Charkaoui v Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 SCR 350; see also European Court of Human Rights (ECHR), "Guide on Article 6 of the European Convention on Human Rights" (30 April 2017), online: <http://www.echr.coe.int/Documents/Guide_Art_6_ENG.pdf> (rights under Article 6(1) include (1) access to a court, which is real and effective; (2) a hearing before an independent and impartial tribunal established by law; (3) that this hearing be public in nature and within a reasonable time; (4) that it present a real opportunity for the case to be made; and (5) that there be a reasoned decision).

prosecuting terrorists where national security information is at risk of disclosure. This information was not otherwise available. As such, primary research was critical for understanding how those who investigate and practice law in the shadows work with those who prosecute terrorists in open court.

The author sought and received approval to conduct in person interviews from the University of Ottawa's Social Sciences and Humanities Research and Ethics Board.[35] Research subsequently began in Canada with conversations with Department of Justice counsel, Bill Boutzouvis and Debra Robinson. They were asked about their work with UK prosecutors during the Operation Crevice trial of five members of a terrorist cell with Canadian connections, and to discuss any advantages they perceived to the UK evidentiary system.[36] Experienced Special Advocates, John Norris, and the Honourable Justice Francois Dadour, were also engaged for their perspective on the UK's application of public interest immunity in comparison to the regime under the *Canada Evidence Act*; both men previously travelled overseas to share lessons learned and best practices with their British counterparts.

Next, the author travelled to London in November 2017. Three lawyers from the Counter-Terrorism Division of the Crown Prosecution Service, Jess Hart, Karen Stock and the division head Mari Reid, were interviewed and agreed to have their comments recorded and transcribed for attribution in this article. Interviews were also conducted and recorded for attribution with the First Senior Treasury Counsel at the Criminal Court Mark Heywood, QC and Senior Treasury Counsel Louis Mably, QC.[37] As Senior Treasury Counsel, these barristers argue the most serious criminal offences at London's Central Criminal Court, and both have extensive experience prosecuting terrorism offences. Martin Chamberlain, QC, a Special Advocate and human rights barrister, was also interviewed about his opinions and experience in closed material proceedings.[38] Finally, David

---

35 University of Ottawa, Social Science and Humanities REB, Ethics Approval Notice, No 03-17-01 (approved 8 May 2017).

36 "Five Get Life over UK Bomb Plot," *BBC News* (30 April 2007), online: <http://news.bbc.co.uk/2/hi/6195914.stm>.

37 Attorney General's Office, "New First Senior Treasury Counsel announced" (5 November 2015), online: <https://www.gov.uk/government/news/new-first-senior-treasury-counsel-announced>.

38 For comments by Martin Chamberlain on Closed Proceedings, see "Special Advocates

Anderson, QC, the former Independent Reviewer of Terrorism Legislation met with the author to share his perspective of MI5 and police cooperation, and the potential impact of the new *Investigatory Powers Act*[39] on national security investigations.[40] Unfortunately, while some members of the Metropolitan Police's counterterrorism unit were willing to meet with the author, their heavy workload did not permit in-person interviews; limited information was exchanged via email.

All persons interviewed consented to being identified by name and title. Universally, those in London stand by and were proud of the work they are doing to counter and prosecute terrorism, and were hopeful that the lessons learned by the UK could assist Canada in overcoming the ongoing intelligence to evidence dilemma.

III. The History of the Problem

A. The Difference between Intelligence and Evidence

The I2E problem is typically explained as one rooted in the divergent mandates of Canada's primary national security agencies: the Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS or "the Service").

Prior to the creation of CSIS in 1984, the RCMP's Security Service was responsible for both domestic security intelligence and national security policing. Following a series of scandals and failures by the Security Service in the 1970s and 80s, the 1981 *Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police*[41] recommended that the responsibility for collecting intelligence be stripped from the RCMP and entrusted to a civilian intelligence agency with a clearly defined legislative mandate.[42]

---

and Fairness in Closed Proceedings" (2009) 28:3 CJQ 314.

39 *Investigatory Powers Act 2016* (UK), c 25.

40 For David Anderson's report on the legislation, see *A Question of Trust: Report of the Investigatory Powers Review* (June 2015), online: <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>.

41 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, Second Report, vol 2 (Ottawa: PCO, 1981) [*Macdonald Commission*].

42 *Ibid* at 428, 753; Canadian Security Intelligence Service, "History of CSIS" (May 2014), online: <https://www.csis-scrs.gc.ca/hstrrtfcts/hstr/index-en.php>; Phillip Rosen,

The Government of the day heeded the advice of the MacDonald Commission and introduced legislation establishing a new civilian national security agency. Separating the Security Service from the RCMP was meant to prevent a single agency from having "too much, or inadequately controlled power"[43] thereby becoming a threat to individual rights.[44]

In 1983, the report of the Special Senate Committee established to review Bill C-157, the *Canadian Security Intelligence Service Act* (*CSIS Act*)[45] highlighted the differences between security intelligence and law enforcement:

> The differences are considerable. Law enforcement is essentially reactive. While there is an element of information-gathering and prevention in law enforcement, on the whole it takes place after the commission of a distinct criminal offence. The protection of security relies less on reaction to events; it seeks advance warning of security threats, and is not necessarily concerned with breaches of the law. Considerable publicity accompanies and is an essential part of the enforcement of the law. Security intelligence work requires secrecy. Law enforcement is "result-oriented", emphasizing apprehension and adjudication, and the players in the system- the police, prosecutors, defence counsel, and the judiciary- operate with a high degree of autonomy. Security intelligence is, in contrast "information-oriented"... Finally, law enforcement is a virtually "closed system with finite limits-commission, direction, apprehension, adjudication. Security intelligence operations are much more open-ended. The emphasis is on investigation, analysis and formulation of intelligence.[46]

Since its establishment, the primary mandate of CSIS is the collection of security intelligence to investigate defined threats and advise the Government on matters related to the security of Canada.[47] The Service's

---

Library of Parliament, "The Canadian Security Intelligence Service" (24 January 2000) [84-27E].

43 *Debates of the Senate*, 32nd Parl, 1st Sess (3 November 1983) at 6131 (Michael Pitfield).

44 *Ibid.* See also Senate, Special Committee on the Canadian Security Intelligence Service, *Report of the Special Committee of the Senate on the Canadian Security Intelligence Service, Delicate balance: A Security Intelligence Service in a Democratic Society* (November 1983) [*Pitfield Report*].

45 *Canadian Security Intelligence Services Act*, RSC 1985, c. C-23 s 12 [CSIS Act].

46 *Pitfield Report*, *supra* note 44 at 6 (for early discussions on the CSIS mandates, see the five-year review of the CSIS Act: House of Commons, Special Committee on the Review of the CSIS Act and the Security Offences Act, *In flux but not in crisis: a report of the House of Commons Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act* (September 1990).

47 CSIS Act, *supra* note 45. "Threats to the security of Canada" is defined in section 2 of

role is intentionally proactive rather than reactive, and to fulfil its mandate CSIS may collect and analyze information gathered from open and closed sources. Importantly, CSIS does not collect information with the aim of using it to support a criminal conviction, but the Service may share information related to criminal activities with law enforcement.[48]

As a security intelligence service, every action taken by CSIS regardless of the threat under investigation is governed by three key considerations, or perhaps more accurately, three preoccupations. First, unlike typical policing, security intelligence has national and international dimensions. The threat actors, influences, consequences and theatres of operation demand liaison and information sharing with foreign and domestic partners of all types, often under the demand for secrecy.[49] As a "net importer of intelligence"[50] maintaining strong relationships of trust with these partners is vital to the Service's success.[51] Second, the constant fear of penetration by a foreign agency or threat actor demands unrelenting vigilance and creates

---

the Act as (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage; (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person; (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious, or ideological objective within Canada or a foreign state; and (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada; but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

48 *Ibid* ss 14(b), 19(2)(a); *Pitfield Report*, *supra* note 44 at 6.

49 *Macdonald Commission*, *supra* note 41 at 693. For a description of the "Originator Control" principle and some of Canada's intelligence sharing agreements, see Craig Forcese, "The Collateral Casualties of Collaboration" in Hans Born, Ian Leigh & Aidan Wills, eds, *International Intelligence Cooperation and Accountability* (New York: Routledge, 2011).

50 *Charkaoui v Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 SCR 350 at para 68.

51 *Ibid*; Evidence to Senate Standing Committee on National Security and Defence, 39th Parl, 1st Sess (26 March 2007) (Margaret Bloodworth, National Security Advisor); Kent Roach, *Comparative Counter-Terrorism Law* (Toronto: Cambridge, 2015) at 771; Kent Roach, "Permanent Accountability Gaps and Partial Remedies" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa, 2015) at 174.

an obsessive need to safeguard employees, sources and investigative techniques.[52] Third, the ultimate aim of a security intelligence organization is not the public recognition of success or to provide a sense of security to citizens. The aim is the collection of information about people and organizations who seek to obscure their true intent, necessitating the careful use of deceit, manipulation and intrusive technology without violating the rights and freedoms the agency has been established to protect.[53]

While the responsibility for national security intelligence was transferred to CSIS in 1984, the RCMP retained jurisdiction over national security law enforcement.[54] Following the attacks on 9/11, the RCMP established Integrated National Security Enforcement Teams (INSET) across the Country to "collect, share and analyze information and intelligence that concern threats to national security and criminal extremism/terrorism."[55] The aim of these teams is "to reduce the threat of terrorist criminal activity in Canada and abroad by preventing, detecting, investigating, and gathering *evidence* to support the prosecution of those involved in national security-related criminal acts."[56] Unlike the security intelligence collected by CSIS, evidence is information collected by the RCMP to advance a police investigation, support the laying of criminal charges, and secure a conviction.[57]

---

52 *Macdonald Commission, supra* note 41 at 693; Senate, Special Committee on Terrorism and Public Safety, *Report* (1987) at 41 (Chair Hon William Kelly); *Henrie v Canada (Security Intelligence Review Committee),* [1989] 2 FC 229, 53 DLR (4th) 568 at 577–578, aff'd (1992), 88 DLR (4th) 575, 140 NR 315 (FCA).

53 *Macdonald Commission, supra* note 41 at 693–694; Solicitor General Canada, *People and Process in Transition Report to the Solicitor General by the Independent Advisory Team on CSIS* (October 1987) at 5.

54 *Security Offences Act*, RSC 1985, c S-7, s 6 (federalizes the prosecution and police role for crimes implicating national security and gives RCMP jurisdiction over the "apprehension of the commission" of these offences).

55 "Security Criminal Investigations Programs" (21 October 2017), online: <http://www.rcmp-grc.gc.ca/nsci-ecsn/index-eng.htm> [*Security Criminal Investigations Programs*]. For more on the growth of the RCMP counter-terrorism intelligence capabilities, see Martin Rudner, "Challenge and Response: Canada's Intelligence Community and the War on Terrorism" (2004) 11:2 Cdn Foreign Policy J 17.

56 *Security Criminal Investigations Programs, supra* note 55.

57 The RCMP's duties are codified in *Royal Canadian Mounted Police Act*, RSC 1985, c R-10, s 18.

To be used at trial, the collection of evidence must comply with constitutional and legislated standards, and law enforcement's adherence to these standards is often the subject of litigation. Consequently, the police and Crown Prosecutors expect that the reliability and significance of the material they have collected will be challenged in open court.[58]

When the collection mandates of the RCMP and CSIS are layered over conventional security threats such as foreign espionage or organized crime, the lines between these organizations' areas of responsibility scarcely intersect. The same cannot be said for terrorism. Unlike most criminal investigations that arise after an offence is committed, investigations into terrorism are designed to stop the bomb from going off. Consequently, various forms of preparatory conduct is criminalized under the *Criminal Code* which, along with the Service's new authority to engage in "threat disruption" activity, has blurred the lines between security intelligence and law enforcement.[59] As a result, CSIS and the information it collects are increasingly drawn into criminal proceedings.

We can anticipate that the growing threat of domestic terrorism and the corresponding shift in both RCMP and CSIS resources towards anti-terrorism will continue to augment the need to use security intelligence as evidence in criminal proceedings.[60] This reality, however, clashes with the

---

58 *Air India Vol 4*, *supra* note 9 at 12, 38; Security Intelligence Review Committee, *Annual Report 1991–1992* (1992) at 9–10.

59 CSIS's threat reduction mandate was introduced in 2015 through Bill C-51 and codified in the CSIS Act, *supra* note 47, s 12.1: "If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat"; see also *Air India Vol 4*, *supra* note 9 at 47; *False Security*, *supra* note 7 at 13. For examples of peremptory or inchoate offences, see *Criminal Code*, *supra* note 14, s 83.02 (Providing or collecting property for certain activities), s 83.03 (Providing, making available, etc., property or services for terrorist purposes), s 83.04 (Using or possessing property for terrorist purposes), s 83.181 (Leaving Canada to participate in activity of terrorist group).

60 Colin Freeze, "RCMP Shelved Hundreds of Organized-Crime Cases After Terror Attacks," *The Globe and Mail* (18 September 2017), online: <https://www.theglobeandmail.com/news/national/mounties-put-hundreds-of-files-on-hold-in-shift-toward-anti-terrorism/article36285597/>. ("INSETS were allotted budgets of $10-million each year shortly after they were created in the early 2000s and soon started overrunning these budgets by hundreds of thousands of dollars. By a decade later, the overruns had increased consistently by $15-million to $20-million, and in 2014 and 2015, after the terrorist attacks that killed the soldiers, the INSETs were overspending by $50-million each year. Last year, the overrun was reduced to $40-million").

Service's preoccupying need to protect its officers, methods, partners, and sources from public scrutiny.

B. I2E: A recognized problem since Air India

To this day the Air India bombing remains the deadliest terrorist attack in Canadian history, and yet, it took almost two decades to bring the perpetrators to trial. When hearings finally commenced in 2003, only three people stood charged. The attack's mastermind, Talsinder Singh Parmar, ultimately plead guilty to manslaughter before the conclusion of the 217 day judge-alone trial; the two others, Ripudaman Singh Malik and Ajaib Singh Bagri were acquitted.[61]

The acquittal of Malik and Bagri resulted from the trial judge's finding that key prosecution witnesses lacked credibility.[62] These witnesses had been CSIS human sources and promised confidentiality. Instead of the anonymity they were assured, they were dragged onto the stand and faced public cross-examination. One of the sources was forced into witness protection after an RCMP error revealed her name.[63] Another potential witness, Tara Singh Hayes, was murdered.[64] Unsurprisingly the testimony of the remaining human sources was reluctant and easily shaken.[65]

Following the trial, the Government struck a commission of inquiry to review the intelligence investigation of the Air India plot, the criminal investigation of the bombing, and the failed prosecutions of the conspirators. One of the Commission's assigned tasks was to examine how Canada could establish "a reliable and workable relationship between security intelligence and evidence that can be used in a criminal trial."[66] Another task was to assess "whether the unique challenges presented by the prosecution of terrorism cases…are adequately addressed by existing

---

61 *Air India Vol 1*, *supra* note 21 at 116; *False Security*, *supra* note 7 at 48–50.

62 *R v Malik and Bagri*, 2005 BCSC 350, 64 WCB (2d) 420; Kent Roach, "The Air India Trial" (2005) 50:3 Crim LQ 213.

63 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy-Post Bombing, Vol 2* (Ottawa: Public Works, 2010) at 221–223 [*Air India Vol 2*].

64 *False Security*, *supra* note 7 at 50.

65 *Air India Vol 2*, *supra* note 63 at 222–224.

66 *Air India Vol 4*, *supra* note 9 at 11.

practices or legislation and, if not, the changes in practice or legislation that are required to address these challenges."[67]

In 2010, the Commission concluded that CSIS had failed to share important information collected after the bombing with the RCMP, and when it did, refused to make collected intelligence available for use in criminal prosecutions. This, the report found, diminished both the quality evidence available at trial and the accused's rights to procedural fairness.[68] Predictably, a key reason cited by the Commission for the break down in the relationship was that information shared by CSIS with the RCMP was inadequately protected, thereby compromising the Service's sources, methods and assessments. Another reason identified was the Service's fear of the Crown Prosecutor's far-reaching disclosure obligations in criminal proceedings.[69]

The Commission's report offered 35 recommendations to improve the relationship between intelligence and evidence, and enhance the efficiency and effectiveness of terrorism prosecutions. However, more than thirty years after the bombing, few if any of the Commission's suggestions have been adopted, and Canada continues to struggle under the weight of inordinately long and complex "mega-trials."[70]

The I2E problem, however, has not been lost on the subsequent Governments. In 2013, a Public Safety report outlining the Harper Government's counter terrorism strategy noted that "[p]rosecuting terrorist activities may engage the relationship between intelligence and evidence, which can represent significant disclosure challenges. Individual rights, such as the right to due process, need to be balanced with the need to protect national security sources and methods."[71] The Report also described the undertaking of an "extensive review of the disclosure process and the role of security intelligence agencies in this process."[72] No public findings and no apparent changes were made as a result of that review.

---

67 *Ibid.*

68 *Air India Vol 1*, *supra* note 21 at 148

69 *Ibid.*

70 Canada, Public Safety, "Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy" (Ottawa: Public Safety, 2013) at 24 ["Building Resilience"]; see also *False Security*, *supra* note 7 at 290.

71 "Building Resilience," *supra* note 70 at 25.

72 *Ibid.*

Next, in the second half of 2016, the Trudeau Government engaged in wide-ranging consultations with Canadian citizens, stakeholders and subject-matter experts on issues related to national security.[73] The green paper published to facilitate these discussions set out the I2E problem and noted:

> [s]ometimes, this means that a criminal court may be unable to hear the national security information – and may need to rely on an unclassified summary instead… This raises the question of whether justice can truly be served in these examples.[74]

In June 2017, the Liberal Government's consultations culminated in the introduction of Bill C-59: *An Act respecting national security matters* which, if passed, will result in the most significant overhaul of the Canadian national security regime since the creation of CSIS. Accompanying the Bill was a *Charter* statement submitted to Parliament by the Attorney General explaining that widespread changes are necessary to ensure that "Canada's national security framework keeps pace with developments in the current threat environment."[75] Noticeably absent from the proposed legislation was any means of resolving the intelligence to evidence problem. Instead, in the summer of 2017, the Government recommitted to further "targeted consultations" on the I2E problem.[76] A consultation paper was circulated, however the results of the process are still outstanding.

Through all of this, Canada has continued to struggle to bring terrorists to trial. Between 2001 and 2015 Canada conducted 21 terrorism prosecutions.[77] The Public Prosecution Service of Canada (PPSC) is

---

73 Canada, Public Safety, *National Security Consultations: What We Learned Report* (Ottawa: Public Safety, 2017) at 1.

74 Canada, Public Safety, *Our Security, Our Rights: National Security Green Paper, 2016* (Ottawa: Public Safety, 2016) at 20.

75 House of Commons, Charter Statement, *Bill C-59: An Act respecting national security matters* (20 June 2017).

76 Government of Canada, "Questions and Answers: Strengthening Security and Protecting Rights," online: <https://www.canada.ca/en/services/defence/nationalsecurity/our-security-our-rights/questions-answers-strengthening-security-protecting-rights.html?wbdisable=true> ("Discussions are now underway with provinces and territories, judges and experts regarding proposals to amend the Canada Evidence Act and other statutes in an effort to "create a national security system of justice in criminal and civil proceedings that protects Canadians while safeguarding their rights").

77 Public Prosecutions Services Canada, "Transition Book" (February 2017), online: <http://www.ppsc-sppc.gc.ca/eng/tra/tr/08.html>; *False Security, supra* note 7 at 317–322.

responsible for national security prosecutions across the country. The PPSC *2016-2017 Report on Plans and Priorities* reinforced the importance of bringing terrorists to trial given "the gravity of the impact of these offences on Canada's national security, international relations and national defence."[78] At the time of the annual report's publication, PPSC was in the midst of prosecuting an additional 17 individuals for terrorism offences and had charges pending against 9 persons located outside of Canada.[79] While this may appear to be a major jump given the number of successful terrorist attacks and publicized attempts in Canada in recent years, it is only a fraction of those persons known to have left this country to engage in terrorist activity abroad. As of February 2016, the Federal government was aware of more than 180 individuals with Canadian connections who were abroad and suspected of engaging in terrorism-related activities or joining terrorist organizations, and 60 who had returned.[80] In November 2017, the Minister of Public Safety confirmed that the number of persons designated as "extremist travellers"[81] who had returned to Canada remained approximately 60 however, since first reported, only 2 of the 60 had been charged with a criminal offence.[82]

---

78 Public Prosecution Service Canada, "Report on Plans and Priorities 2016–17" (accessed 17 October 2017), online: <http://www.ppsc-sppc.gc.ca/eng/pub/rpp/2016_2017/index.html#section_2_2>.

79 *Ibid.*

80 *Criminal Code*, *supra* note 14, s 83.191 (Leaving Canada to facilitate terrorist activity); s 83.201 (Leaving Canada to commit offence for terrorist group); s 83.202 (Leaving Canada to commit offence that is terrorist activity).

81 Public Safety Canada, *2016 Public Report on the Terrorist Threat to Canada* (Ottawa: Public Safety, 2016) at 7.

82 *Ibid*; Robert Fife, "Spy Agencies See Sharp Rise in Number of Canadians Involved in Terrorist Activities Abroad" (23 February 2016), online: <https://beta.theglobeandmail.com/news/politics/sharp-rise-in-number-of-canadians-involved-in-terrorist-activities-abroad/article28864101/?ref=http://www.theglobeandmail.com&>; Daniel Leblanc & Colin Freeze, "RCMP Investigating Dozens of Suspected Extremists Who Returned to Canada," *Globe and Mail* (8 October 2014), online: <http://www.theglobeandmail.com/news/politics/rcmp-investigating-dozensof-suspected-extremists-who-returned-to-canada/article20991206/> (in October 2014, the RCMP was reportedly tracking 90 individuals who intended to travel or had returned from overseas); John Geddes, *MacLeans*, "What Should Canada Do About Returning Jihadists?" (24 November 2017).

IV. DISCLOSURE

A. Canada's Disclosure Regime

In Canada, Crown disclosure in criminal proceedings is a constitutionally protected right governed by common law. The common law rule requires the Crown to disclose all relevant information in its possession and control.[83] The two assumptions underpinning the Crown's disclosure obligation are (1) that the material is relevant to the accused's case otherwise, it would not be in the possession of the Crown; and (2) that the material will comprise the case against the accused.[84]

Crown disclosure includes "any information in respect of which there is a reasonable possibility that it may assist the accused in the exercise of the right to make full answer and defence."[85] It is not limited to material that will be introduced as evidence, and there is no distinction between inculpatory and exculpatory information. The fruits of a criminal investigation are not the property of the Crown but rather the property of the public to be used to ensure justice is done.[86] The defence, on the other hand, is entitled to maintain a "purely adversarial role"[87] and has no duty to assist the prosecution through disclosure.[88]

The constitutional premise for the *Stinchcombe* rule is that failure to disclose information in the Crown's possession impedes an accused's ability to make full answer and defence which is a fundamental principle of justice protected by s. 7 of the *Charter*.[89] Therefore, "[u]nless the information is clearly irrelevant, privileged, or its disclosure is otherwise governed by law, the Crown must disclose to the accused all material in its possession."[90]

---

83 *Stinchcombe, supra* note 16 at 338.

84 *Ibid* at 339. There is, however, a duty to disclose alibi evidence. See *R v Cleghorn*, [1995] 3 SCR 175, 1995 CanLII 63 at para 32.

85 *R v McNeil,* 2009 SCC 3, [2009] 1 SCR 66 at para 17 [*McNeil*].

86 *Stinchcombe, supra* note 16 at 333 (as address in Part IV, the law does, however, provide for limited or delayed disclosure in order to protect privileges and other interests); see CEA, *supra* note 18 at ss 37–39.

87 *Ibid.*

88 *Ibid.*

89 *R v O'Connor*, [1995] 4 SCR 411, 1995 CanLII 51 at para 18 [*O'Connor*]; *Stinchcombe, supra* note 16 at 340.

90 *McNeil, supra* note 85 at para 18.

Even then, claims of privilege are subject to review by the trial judge who, in certain circumstances, may "conclude that the recognition of an existing privilege does not constitute a reasonable limit on the constitutional right to make full answer and defence and thus require disclosure in spite of the law of privilege."[91]

Stinchcombe disclosure is problematic for national security investigations where intelligence is or could be shared with law enforcement. Any intelligence shared with police in the course of investigating terrorist activity will be subject to disclosure unless the Attorney General can justify withholding it on the basis of privilege, most commonly s. 38 of the *Canada Evidence Act*.[92]

Section 38 of the *CEA* sets out a regime for preventing the disclosure of information or documents that contain "sensitive"[93] or "potentially injurious"[94] information. Potentially injurious information is defined in the *CEA* as information that "if it were disclosed to the public, could injure international relations or national defence or national security."[95] Sensitive information refers to "information relating to international relations or national defence or national security that is in the possession of the Government of Canada, whether originating from inside or outside Canada, and is of a type that the Government of Canada is taking measures to safeguard."[96]

This regime will be discussed in more detail in Part III however, it is important to highlight that invoking s. 38 does not guarantee that sensitive or injurious information will be protected from disclosure. The Federal Court judge tasked with hearing the s. 38 application must engage in a three-part test and balancing exercise.[97] First, the designated judge determines that the information subject to disclosure is relevant. Second, would the release of the information be injurious to national security, national defence or international relations? If yes, this is not enough to bar its release. Under the third part of the test, the Judge must find that the public interest in

---

91 *Stinchcombe*, *supra* note 16 at 340.

92 CEA, *supra* note 18, s 38.

93 *Ibid.*

94 *Ibid.*

95 *Ibid.*

96 *Ibid.*

97 *Canada (AG) v Ribic*, 2003 FCA 246 at paras 17-21, [2005] 1 FCR 33 at 17–21 [*Ribic*].

disclosing the information is outweighed by the public interest in protecting it.[98] This final balancing exercise makes it impossible for CSIS to know with any level of certainty whether the information they share with law enforcement will one day become public in a criminal proceeding.

To limit the possibility that their intelligence will be subject to *Stinchcombe* disclosure, CSIS and the RCMP engage in parallel investigations rather than joint operations. This relationship is guided by the "*One Vision 2.0*" framework established by the agencies to reinforce "the importance of collaboration and information sharing, while respecting legislative mandates, in order to facilitate separate and distinct investigations in parallel."[99] This framework specifies that CSIS information shall be shared with RCMP by way of either an advisory letter or a disclosure letter.

Disclosure letters are a means for the Service to share a tip or provide a lead to the police that they may then use to discover or develop evidence of an offence.[100] The Service's authority to share this information is governed by s. 19(2) of the *CSIS Act*. While it is understood that these letters will be subject to disclosure if criminal charges are laid, the information contained therein is not to be used to support an application before the Court for a warrant or arrest.[101] These letters are centrally controlled, and their contents are not to be disseminated beyond the headquarters level of the RCMP.[102]

An advisory letter results from a formal request by the RCMP to use CSIS information in a specified manner.[103] Once provided to the RCMP, the letters can be disseminated at the force's discretion.[104] These letters will often include caveats respecting the use of the information in various proceedings, including the requirement to obtain a sealing order to protect the release of the information when seeking a judicial authorization for a search warrant, wiretap or production order. CSIS also has the opportunity

---

98 *Canada (AG) v Khawaja*, 2007 FCA 388, [2008] 4 FCR 3 at para 8 [*Khawaja*].

99 ATIP Release to Colin Freeze: *CSIS- RCMP Framework For Cooperation, One Vision 2.0*, online: <https://www.theglobeandmail.com/news/national/article31788061.ece/BINARY/na-security-web-document.pdf>.

100 *Ibid.*

101 *Ibid.*

102 *Ibid.*

103 *Ibid.*

104 *Ibid.*

to review any application brought by the RCMP that leverages the information provided in an advisory letter before it is filed with the Court.[105]

Maintaining separate and distinct investigations also serves to prevent CSIS from becoming a party to the Crown's criminal investigation for the purpose of disclosure. The duty to disclose under *Stinchcombe* only extends to material in the possession and control of the Crown, including all material gathered by an investigating police force. Information falling outside the police and prosecutor's investigation is classified as third party material.

1. Third Party Disclosure

PPSC guidelines make clear that information in the possession of other government departments is not to be considered in the possession of the Crown or the investigative agency for disclosure purposes.[106] Only if the Crown "is put on notice or informed of the existence of potentially relevant information in the hands of a third party, including information pertaining to the credibility or reliability of the witnesses in a case"[107] does the Crown have an obligation to make reasonable inquiries with the third party.[108] Other government agencies are not obligated to provide the Crown with the requested information, but the Crown must notify the defence so that they can determine whether to bring an application for the third party records.[109]

The Supreme Court set out the test to obtain third party disclosure in *O'Connor*. First, the onus is on the defence to establish that the records sought are likely relevant, meaning there is a "reasonable possibility that the information is logically probative to an issue at trial or the competence of a witness to testify."[110] If the relevance threshold is met, the records must be produced to the Court who then weighs "the positive and negative

---

105 *Ibid.*

106 Public Prosecution Service of Canada, "Deskbook: Part II: Principles Governing Crown Counsel's Conduct, Principles of Disclosure," s 4.1, online: <http://www.ppsc-sppc.gc.ca/eng/pub/fpsd-sfpg/fps-sfp/tpd/p2/ch05.html#section_4_1>.

107 *Ibid.*

108 *Ibid.*

109 *Ibid.*

110 *O'Connor, supra* note 89 at para 22.

consequences of production with a view to determining whether, and to what extent, production should be ordered."[111] In carrying out this balancing exercise, the court must consider a variety of factors including the accused's right to make full answer and defence, and the reasonable expectation of privacy vested in the records.[112]

So long as the Service's role in a national security criminal investigation is such that CSIS can maintain its status as a third party, information in the possession and control of the Service will be protected from disclosure unless the accused can meet *O'Connor's* higher relevance threshold. However, should CSIS's activities be too closely intertwined with the work of the investigating police force they could be considered a first party, necessitating full *Stinchcombe* disclosure.

A finding that CSIS acted as a first party in a criminal terrorism investigation would create massive risks for the Service. As noted above, the mandate of the Service is much broader than the RCMP's because "an intelligence dossier will naturally contain a range of information, including much that is unsifted or unfiltered, as well as innuendo, hearsay and speculation."[113] CSIS investigates threats rather than specific crimes, and CSIS may collect information where there are "reasonable grounds to suspect" that the information may assist with an investigation into a threat to the security of Canada. By consequence, the Services' investigative holdings regarding a threat connected to the accused would likely extend far beyond the scope of a criminal investigation. However, in order to comply with *Stinchcombe,* it is possible that much of the CSIS file, while unrelated to the criminal charge in and of itself, would not be *clearly irrelevant* to the initial investigative threshold, the credibility or reliability of witnesses or informants, or the basis for securing an early search warrant or wiretap authorization, thereby necessitating its disclosure.

---

111 *Ibid* at para 137.

112 *Ibid* at para 31.

113 Stanley Cohen, *Privacy, Crime and Terror Legal Rights and Security in a Time of Peril* (Toronto: LexisNexis Canada, 2005) at 404.

B. The UK Disclosure Regime

1. Crown Disclosure Duty

The UK disclosure regime is codified in Part II of the *CPIA*[114] and fully detailed in an associated *Code of Practice*.[115] Applying the *Code of Practice* is only mandatory for police investigations "with a view to it being ascertained whether a person should be charged with an offence or is guilty of an offence so charged."[116]

Similar to the test for relevance in Canada, relevant material is defined in the *Code of Practice* as anything that appears "to have some bearing on any offence under investigation or any person being investigated or on the surrounding circumstances unless it is incapable of having any impact on the case."[117] However, unlike the Canadian regime, what must be disclosed to an accused is not synonymous with what is "relevant." Aside from the materials the Crown will be relying on to make their case against the accused, prosecutors are only obligated to disclose information "which might reasonably be considered capable of undermining the case against the accused, or of assisting the case for the accused"[118] regardless of whether that material would be admissible at trial.[119] This is known as the "disclosure test" and applies to material the prosecution either has in their possession or has inspected. The prosecution has an ongoing responsibility to apply this test to unused material throughout the proceedings.[120]

Material that is deemed to be relevant but will not form part of the prosecution's case is classified as "unused material."[121] This material is listed in a detailed schedule by a police officer assigned to serve as the case's

---

114 CPIA, *supra* note 17.

115 Canada, Ministry of Justice, *Criminal Procedure and Investigations Act 1996 (Section 23(1)) Code of Practice* at para 2.1 [*Code of Practice*].

116 CPIA, *supra* note 17, s 22(1).

117 *Code of Practice*, *supra* note 115, s 2.1.

118 CPIA, *supra* note 17, s 3.

119 *Ibid*, ss 3, 7(a).

120 David Corker & Stephan Parkinson, *Disclosure in Criminal Proceedings* (Oxford: Oxford University Press, 2009) at 86 (originally there were two tests for disclosure, one at the initial stage and one following defence disclosure; the tests were unified under the *Criminal Justice Act 2003*).

121 *Code of Practice*, *supra* note 115 at para 7.

"disclosure officer."[122] Prosecutor's work with the disclosure officer early and often to ensure they are aware of the issues involved in the case as it progresses to trial.[123] The prosecutor is allowed to rely on this schedule without inspecting the material except where the disclosure officer believes the unused material may satisfy the test for disclosure.[124] The schedule of unused material is provided to the defence for their review.[125]

The House of Lords had the opportunity to opine on the Crown's disclosure obligation in *R v H and C*.[126] The House found that "if material does not weaken the prosecution case or strengthen that of the defendant there is no requirement to disclose it."[127] The House was categorical that "[n]eutral material or material damaging to the defendant need not be disclosed and should not be brought to the attention of the court."[128] Prosecutors are instructed against being lax in their approach to disclosure; the UK justice system, recognizes the Crown Court, is not well served if it is overburdened by erroneous or wholesale disclosure.[129]

In the context of national security investigations leading to a criminal charge, the result of the House's interpretation and the Court's guidelines is that security intelligence in the possession of the police or Crown need not be disclosed unless the Crown intends to rely on it or the material would weaken the prosecution's case.

In practice, Crown disclosure for terrorism offences is overseen by a dedicated unit of lawyers who comprise the Crown Prosecution Service's

---

122 *Ibid* at para 2.1.

123 Interview of Mari Reid, Unit Head Counter Terrorism, Special Crime and Counter Terrorism Division, Crown Prosecution Service (9 November 2017).

124 *Code of Practice, supra* note 115 at paras 7.1–7.3 (information provided by an accused person which indicates an explanation for the offence with which he has been charged; any material casting doubt on the reliability of a confession; any material casting doubt on the reliability of a prosecution witness; any other material which the investigator believes may satisfy the test for prosecution disclosure in the Act).

125 *Ibid* at para 10.1.

126 *R v H; R v C*, [2004] UKHL 3, [2004] 2 AC 134 [*H and C*].

127 *Ibid* at para 35.

128 *Ibid*.

129 Court and Tribunals Judiciary, "Disclosure: A Protocol for the Control and Management of Unused Material in the Crown Court" (April 2010) at para 3, online: <https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Protocols/crown_courts_disclosure.pdf> [*Crown Court Disclosure Protocol*].

Special Crimes and Counter Terrorism Division. The Counter Terrorism Division was established in 2011 in acknowledgement of both the size and complexity of terrorism prosecutions, and the special considerations needed when managing cases that involve sensitive material and security intelligence.

Seasoned CPS Counter Terrorism lawyers repeatedly stressed that prosecuting these cases demands early consultation with the disclosure officer to identify all of the sources of disclosure, especially where there may be material held by local police forces, foreign law enforcement, and various security agencies.[130] Wherever possible, CPS counsel prefer to brief investigating police agencies before charges are laid if there is any risk that the security agencies have had contact with the suspect.[131]

Additionally, in terrorism cases, CPS will always contact MI5 (the UK's security intelligence agency), MI6 (the foreign intelligence agency) and GCHQ (the signals intelligence agency). As a matter of course CPS will provide the agencies with a written case summary, a list of proposed charges, and request to review any material the agencies hold in relation to the accused. Any identified material is reviewed with a view to (a) possibly using the collected intelligence as evidence, and (b) determining if it meets the disclosure test. While the material remains at all times in the control of the security services, once reviewed by CPS that material is considered "prosecution material" for the purpose of scheduling, and the disclosure test applies.[132]

CPS prosecutors stress the need for constant review, guidance and dialogue between themselves, the disclosure officer, the investigating officer and partner agencies. The issues in terrorism trials can be very complicated, and by consequence the application of the relevance standard and disclosure test can evolve dramatically from investigation to trial, resulting in the need to release additional materials.[133]

Another significant consideration when handing disclosure under the UK regime is the statutory time limits imposed on the Crown to bring cases

---

130 Interview of Jess Hart, Counsel, Special Crime and Counter Terrorism Division, Crown Prosecution Service (9 November 2017).

131 Interview of Mari Reid, *supra* note 123.

132 Interview of Jess Hart, *supra* note 130.

133 Interview of Karen Stock, Senior Counsel, Special Crime and Counter Terrorism Division, Crown Prosecution Service (9 November 2017).

to trial. Under the *Prosecutions of Offences Act*,[134] the Crown must bring an accused charged with an indictable offence to trial 182 days following the day after the court appearance when the defendant was first remanded.[135] While applications may be made in order to extend this timeline, the Crown must demonstrate "good and sufficient cause"[136] and that they have executed their responsibilities with "all due diligence and expedition."[137]

2. Sensitive Material

The *CPIA* sets out a separate process for handling unused "sensitive material."[138] If a disclosure officer believes the disclosure of information "would give rise to a real risk of serious prejudice to an important public interest"[139] it is listed on a second schedule that is not provided to the defence. The material, however, must be disclosed to the prosecutor who, having an understanding of the full investigation and legal issues, is ultimately responsible for confirming that it is listed on the proper schedule.[140]

Factors that must be considered when making this assessment are listed in the *Crown Disclosure Manual* and include, the ability of the security and intelligence agencies to protect the safety of the UK; the willingness of foreign sources to continue to cooperate with UK security and intelligence agencies; the impact on human sources and confidential informants; and the protection of secret and covert methods of investigation.[141]

---

134 *Prosecution of Offences Act 1985*, 1985 (UK), c 23.

135 *Ibid*, s 22; Crown Prosecution Service, "Legal Guidance: Custody Time Limits," online: <http://www.cps.gov.uk/legal/a_to_c/custody_time_limits/>.

136 *Prosecution of Offences Act 1985*, *supra* note 134, s 22.3.

137 *Ibid.*

138 *Code of Practice*, *supra* note 115 at para 2.1.

139 *Ibid.*

140 Corker & Parkinson, *supra* note 120 at 53; Interview of Jess Hart, *supra* note 130.

141 Crown Prosecution Service, "Legal Guidance: Disclosure Manual" at para 8.4, online: <http://www.cps.gov.uk/legal/d_to_g/disclosure_manual/> [*CPS Disclosure Manual*]. See also para 8.8, which states, "The police and the CPS must always take care to protect intelligence information and information given to the police in confidence. That will be so whether or not it is thought likely that the court will order its disclosure. If the investigator is unsure whether information was given in confidence, the position should be clarified with the person who provided the information."

Should sensitive material satisfy the disclosure test the prosecutor must consider whether, through its release, the "public interest may be prejudiced either directly or indirectly through incremental or cumulative harm."[142] If so, consultation with the police and security services is necessary to determine if it is possible to disclose the material in a way that would be fair to the defence and not compromise the identified public interest. If no compromise is available through the provision of summaries, extracts, redactions, or the admission of facts, the prosecutor must withhold the disclosure on public interest grounds and seek a ruling from the court on the applicability of public interest immunity.[143] Alternatively, they may abandon the case.

The *CPS Disclosure Manual* reaffirms that sensitive neutral material or material damaging to the accused need not be disclosed.[144] Crown Prosecutors alone determine what does and what does not meet the test for disclosure, and thus what sensitive material is at risk of being released. This discretion is the key to the entire intelligence to evidence process.

Prosecutors interviewed for this report were committed to their duty and to applying the disclosure test fairly. This, I heard frequently, may nevertheless involve clever consideration of the facts and issues to identify ways of limiting the *need* for disclosure. This is done pre-charge by deciding not to lay certain charges, charging a lesser offence, or narrowing the dates to which charges apply to obviate the disclosure of sensitive material from earlier phases of an investigation that may have been more intelligence driven.

As an example, a Senior CPS prosecutor described a complex terrorism investigation where there was sufficient evidence to support the charge of "preparation of a terrorist attack" under the *Terrorism Act 2006*.[145] Bringing

---

142 *CPS Disclosure Manual, supra* note 141 at para 8.14.

143 *Ibid* at para 8.22; *Code of Practice, supra* note 115 at para 10.5: "If a court concludes that an item of sensitive material satisfies the prosecution disclosure test and that the interests of the defence outweigh the public interest in withholding disclosure, it will be necessary to disclose the material if the case is to proceed. This does not mean that sensitive documents must always be disclosed in their original form: for example, the court may agree that sensitive details still requiring protection should be blocked out, or that documents may be summarized, or that the prosecutor may make an admission about the substance of the material under section 10 of the Criminal Justice Act 1967."

144 *Ibid* at para 8.23.

145 *Terrorism Act 2006* (UK), c 11.

those charges, however, might require widespread disclosure of sensitive material which could reveal a human source.[146] To avoid these risks CPS would charge the target with a lesser offence such as "encouragement of terrorism" that could be proven without jeopardizing the source or future investigations.[147]

In other circumstances where the Prosecutor believes that security intelligence has a high evidentiary value and may be crucial to meeting the Crown's burden of proof, CPS will provide the security service with a legal opinion as to why the information is important to the prosecution. That opinion will then be assessed by the Services in terms of national security.[148]

This can also arise in circumstances where the police are aware that security intelligence exists and they want to use that intelligence in interviews or as evidence to substantiate a charge where an accused is being held in investigatory detention.[149] In such instances, CPS will be engaged to assess what implications the use of that intelligence may have on disclosure requirements, potential charges, the length of sentence that may be sought, etc. Pre-charge, the message stressed by CPS with MI5 is that this information, once permitted to be converted into and used as evidence, is unlikely to be leveraged just once: "once it's released it's there and it's out there, and if you've got more material of this sort of nature we'll be coming back for it."[150]

The more serious the case, CPS counsel confirmed, the more likely the Security Service will consent to the use of their intelligence as evidence,[151] and to become "overtly involved in a prosecution."[152] Once that commitment is made, noted First Senior Treasury Counsel, Mark Heywood, "a careful decision-making process leads to identifying what that evidential material is, and also considering the mechanisms by which it can be created as evidence and then deployed."[153]

---

146 Interview of Karen Stock, *supra* note 133; the offence is codified in *Terrorism Act* 2006, *supra* note 145, Part 1, s 5.

147 *Terrorism Act* 2006, *supra* note 145, Part 1, s 1.

148 Interview of Karen Stock, *supra* note 133.

149 *Ibid.*

150 *Ibid.*

151 *Ibid.*

152 Interview of Mark Heywood, QC, First Senior Treasury Counsel (8 November 2017).

153 *Ibid.*

Under the UK regime, disclosure does not necessarily demand disclosure of the underlying material, it is the *information* and not the original documents, notes or recordings that must be disclosed.[154] "There is no proscribed form for making disclosure" noted Louis Mably, a senior barrister who has prosecuted several high profile terrorism cases, "it just has to be effective disclosure."[155] This means that post-charge CPS can tailor the need for disclosure by admitting facts or conceding legal issues. Material may also be edited or summarized in a disclosure notice to ensure the information that meets the disclosure test is communicated without jeopardizing the sensitive techniques, sources or partners who were the source of that information.

A source report was used by Senior CPS Prosecutor Karen Stock to exemplify this technique. Ms. Stock noted that should the content of a source report potentially undermine a fact asserted by the Crown, the name and identifying information of the Source could be edited out of the report to allow for its disclosure.[156] She described the conversations between CPS and the agencies on such a matter as a "negotiation" or "consultation," but one that must be agreed upon by all parties. "If everyone is in agreement,"[157] confirmed another CPS Counsel, "that's usually the best way forward. If you can't agree to that then the two options are either a PII application to protect and withhold the information, or drop the case…It's a stark contrast if you can't find some kind of compromise."[158]

As noted above, the Crown has a continuing obligation to release information that becomes disclosable. In practice, fulfilling this obligation falls to the prosecuting barrister; CPS simply does not have the resources for counsel to be present at all stages of a trial.[159] Consequently, barristers will be assigned to terrorism cases early and will review important and potentially problematic sensitive material so that they can work with CPS to develop a trial strategy to avoid raising intelligence to evidence issues.[160] Conventionally two barristers will be assigned to complex cases, and the

---

154 *Ibid.*

155 Interview of Louis Mably, QC, Senior Treasury Counsel (8 November 2017).

156 Interview of Karen Stock, *supra* note 133.

157 Interview of Jess Hart, *supra* note 130.

158 *Ibid.*

159 Interview of Mark Heywood, *supra* note 152; interview of Karen Stock, *supra* note 133.

160 Interview of Mari Reid, *supra* note 123.

junior instructed counsel is responsible for staying abreast of any need for additional disclosure or further investigation throughout the duration of the trial.[161]

Of utmost importance to the entire process is that the barristers are made aware of all of the relevant material and present the criminal case consistently with the intelligence case. Without this awareness, a barrister may inadvertently create disclosure problems by asserting facts too forcefully or in a manner unsupported by the broader national security investigation.[162] The barrister must not only be informed and capable of identifying when the Crown's duty to disclose has been engaged, but must also avoid making allegations or questioning assertions that result in additional material becoming disclosable to the accused.[163] To avoid "a disclosure car-crash,"[164] explained Mark Heywood, the case must be "set on a course which is not going to inadvertently engage material held by the agencies."[165]

3. Defence Disclosure Obligation

In the UK, both the prosecution and the defence must respect the overriding objective that the criminal case be dealt with justly. The *Criminal Procedure Rules* codify that dealing with a criminal case justly entails:

A) acquitting the innocent and convicting the guilty;
B) dealing with the prosecution and the defence fairly;
C) recognising the rights of a defendant, particularly those under Article 6 of the European Convention on Human Rights;
D) respecting the interests of witnesses, victims and jurors and keeping them informed of the progress of the case;
E) dealing with the case efficiently and expeditiously;
F) ensuring that appropriate information is available to the court when bail and sentence are considered; and
G) dealing with the case in ways that take into account—
    a. the gravity of the offence alleged,
    b. the complexity of what is in issue,
    c. the severity of the consequences for the defendant and others affected, and

---

161 Interview of Mark Heywood, *supra* note 152.

162 Interview of Jess Hart, *supra* note 130.

163 Interview of Karen Stock, *supra* note 133.

164 Interview of Mark Heywood, *supra* note 152.

165 *Ibid.*

d. the needs of other cases.[166]

Importantly, all parties are obligated to assist the court in the early identification of real issues.[167]

Both defence and prosecution are also obliged to present evidence, whether disputed or not, in the shortest and clearest way; to limit delay and avoid unnecessary hearings; and to co-operate in the progression of the case.[168] Where the parties have not complied with the *Criminal Procedure Rules* the Court may order costs against the offending party, refuse to allow a party to introduce evidence or draw adverse inferences from the late introduction of an issue or evidence.[169]

In order to ensure the defence meets this duty and the overriding objective is met, they must file a defence statement with the prosecutor and the court. The purpose of this statement is to prevent ambush defences, encourage guilty pleas or discontinuances by the prosecution, facilitate better trial preparation, and generally improve the efficiency of the court system.[170] "The trial process" notes the *CPS Disclosure Manual*, "is not well served if the defence make general and unspecified allegations and then seek far-reaching disclosure in the hope that material may turn up to make them good."[171] What's more, in the UK, it is widely accepted that "concealment of evidence until a late stage by either side necessarily leads to the jury being unable to assess the weight or probative quality of such evidence."[172]

The *CPIA* stipulates that a defence statement must set out in writing the nature of the accused's defence, including any particular defences on which he intends to rely; the facts at issue with the prosecution and why; any point of law he wishes to advance and any authority he intends to rely on in support of that point.[173] Furthermore, any defence statement that raises an alibi must provide the particulars of any witness who is able to give

---

166 Canada, Ministry of Justice, *Criminal Procedure Rules 2015*, SI 2015/1490, r 2.

167 *Ibid*, r 3.3.

168 *Ibid*.

169 *Ibid*, r 3.5.

170 Ian Dennis, *The Law of Evidence*, 5th ed (London, UK: Sweet & Maxwell, 2013) at 364.

171 *CPS Disclosure Manual*, *supra* note 141 at para 15.

172 Steve Unglow, *Evidence Text and Materials* (London, UK: Sweet & Maxwell, 1997) at 319.

173 CPIA, *supra* note 17, s 6(a)(1).

evidence in support of the alibi, or may be of assistance in identifying any such witness.[174] The statement must be updated as required.[175]

Importantly, a defence statement is deemed a statement of the accused, and can be leverage by the prosecution at trial if it contains admissions or inconsistencies with the accused's testimony.[176] Finally, the defence has a duty to provide the court and the prosecution detailed particulars of any witness they intend to call at trial.[177]

Only after the defence statement is served may defence counsel make an application for additional prosecution disclosure. The application must set out the reasonable grounds to believe that the prosecution has the requested material and that is meets the test for disclosure under the *CPIA*.[178]

The *CPS Disclosure Manual* notes that the defence statement enhances the prosecution's ability to (1) make an informed decision about whether the remaining unused material meets the disclosure test; or (2) whether it is necessary to make further investigative enquiries.[179] It is also crucial to the Crown's ability to bring the case to trial in an expedient manner by narrowing down and focusing on the issues in dispute. This is especially true in complex cases or where the investigation entails the search of an accused's personal electronic devices which have the potential to yield hundreds of thousands of pages of information subject to the same principles of disclosure. [180]

A CPS lawyer illustrated this point by describing a case where a man charged with attempting to leave the UK to join the Islamic State. A search of his computer based on curated search terms revealed "mindset" material. The list of search terms and the material found was then disclosed to the defence.[181] The statement of defence subsequently asserted that the accused had an academic interest in gathering material regarding specific research

---

174 *Ibid*, s 6(a)(2).

175 CPIA, *supra* note 17, s 6(b).

176 Dennis, *supra* note 170 at 62.

177 CPIA, *supra* note 17, s 6(c).

178 *Rules of Criminal Procedure 2015*, r 15.5.

179 *CPS Disclosure Manual*, *supra* note 141 at para 15.5.

180 *Ibid* (see c 30, "Digital Guidance," and Appendix H, "The Use of Keyword Searches and Digital Evidence Recovery Officers").

181 Interview of Jess Hart, *supra* note 130.

questions. As a result, the Crown developed a second set of search terms with defence counsel to capture material related to the accused's research interest. This material was also disclosed.

All CPS counsel interviewed agreed that in the past five years there has been a noticeable improvement in the level of defence engagement in national security cases, specifically as it relates to complying with defence disclosure obligations and narrowing issues for trial. They described the shift as a "culture change," which one lawyer credited to the presence of a High Court judge designated to hear terrorism cases at the initial case management conference and throughout all pre-trial proceedings.[182]

4. Third Party Disclosure

The prosecutor's duty to disclose is limited to material that is obtained, generated or examined in the course of an investigation. The *CPIA* makes clear that material held by third parties, including other government and public bodies, is not subject to disclosure in criminal proceedings.[183] The *CPS Disclosure Manual* also states categorically that UK security and intelligence agencies "are third parties under the *CPIA 1996*. They are not deemed to be 'investigators'."[184]

However, under the *CPIA*, an investigator has a duty to pursue all reasonable lines of enquiry.[185] Senior Treasury Counsel referred to this as "the duty to gather."[186] Consequently, if law enforcement or the Crown has reason to believe that a Government department has material that may be relevant to an issue in the case, reasonable steps should be taken to identify and consider such material.[187] What is reasonable will vary from case to case,[188] nevertheless, the *CPS Disclosure Manual* states:

> Where the Agencies believe that they have information (including documents), which may be relevant to the investigation or prosecution of a criminal offence or to the defence, they have a general professional duty to draw this fact to the

---

182 Interview of Karen Stock, *supra* note 133.

183 Corker & Parkinson, *supra note* 120 at 91.

184 *CPS Disclosure Manual*, *supra* note 141 at para 33.2 (examples of other investigating agencies include immigration authorities and foreign police officers).

185 CPIA, *supra* note 17, s 23(1).

186 Interview of Mark Heywood, *supra* note 152.

187 *CPS Disclosure Manual*, *supra* note 141 at para 4.

188 *Ibid.*

> attention of the investigator or prosecutor. Furthermore, the Agencies have a duty to support the administration of justice by ensuring that investigators and prosecutors are given full and proper assistance in their search for relevant material.[189]

Should the Crown be denied access, they must consider "what if any further steps might be taken to obtain the material or inform the defence."[190]

Therefore, if the prosecutor fulfills their obligation "to gather" the defence should never have to make a third party disclosure application from another government agency. Theoretically, an application could be made of another government department, but in practice the prosecutors wants to "own" and control the disclosure process limit unnecessary litigation, and prevent the defence from having a legitimate argument that third party disclosure should be compelled.[191]

C. Practical Implications

Testifying before the Canadian Senate, Joe Fogarty remarked that the UK's enactment of the *CPIA* enabled the sharing of information by national security teams and law enforcement and protected that information from "unnecessary disclosure, the effect of which has improved the operational relationships between the services because it has established a sense of certainty when carrying out their respective mandates."[192]

In Canada, terrorism prosecutions are likely to involve a variety of satellite hearings on issues tied to intelligence to evidence i.e.: the adequacy of disclosure, third party disclosure, or the unsealing of a confidential appendix to a warrant. Every instance creates uncertainty and risk for CSIS. The result: parallel investigations.

Conversely, in the UK, the only time disclosure is litigated in the courtroom is where the defence and the Crown are unable to agree on whether a scheduled piece of unused material meets the disclosure test. As noted above, in such an instance the defence is required to make an application under s. 8 of the *CPIA*. Often, remarked one CPS lawyer, the making of the application resolves the issue before being heard by the trial

---

189 *Ibid* at para 33.8.

190 *CPS Disclosure Manual*, *supra* note 141, Forward at para 50.

191 Interview of Louis Mably, *supra* note 155; interview of Mark Heywood, *supra* note 152.

192 Evidence of Joe Fogarty, *supra* note 28.

judge. This is because in having to enunciate in writing why certain material would assist the defence or undermine the prosecution, the issues is clarified for the prosecution who then agrees to the additional disclosure or resolves the matter through the admission of facts, etc.[193]

The practical effect of the Crown's control over disclosure is that police and intelligence officers can readily share information. To illustrate this point, consider a scenario where MI5 has human source intelligence that gives them reason to believe that a target of investigation is planning to detonate a bomb at a tube station one particular morning in London. This intelligence is passed from MI5 to the Metropolitan police who attend at the tube station. The police identify the subject, find explosives in his possession and arrest him. How the police knew to look for the accused in the station on that date is not subject to disclosure unless the prosecution concludes that something about the human source or the information they provided would undermine the Crown's case. The prosecution has a duty to review the sensitive intelligence material in order to make this assessment, but the defence is prohibited from making a third party application for the disclosure of MI5's investigative holdings. If the defence makes a s.8 application to have the judge determine whether the relevant intelligence is disclosable, the prosecution can present the intelligence investigation to the Judge *ex parte* in order to demonstrate that, in the context of the entire case, the material does not assist the accused.[194] If the judge denies the defence's application, at trial the prosecution simply presents to the jury that on the day in question the police had reason to believe the accused was planning an attack on the tube station, and when located in the area he was found in possession of explosives. "We wouldn't necessarily produce any evidence of why the police happened to be there,"[195] said CPS Counsel, "Why does it matter? What does that matter to the offence? … Why does the jury need to know what specifically told them to go to that tube station unless there is something undermining about that?"[196]

This narrow approach to disclosure is not without flaws, and can and has led to miscarriages of justice. In July 2017, the Crown Prosecution Service Inspectorate and the Inspectorate of Constabulary published a joint

---

193 Interview of Jess Hart, *supra* note 130.

194 *Ibid*; interview of Karen Stock, *supra* note 133.

195 Interview of Jess Hart, *supra* note 130.

196 *Ibid*.

report entitled: *Making it Fair: The Disclosure of Unused Material in Volume Crown Court Cases*.[197] The report found that 22% of police schedules reviewed were wholly inadequate. It also concluded that prosecutors failed to comply with the Attorney General's guidelines and challenge police when schedules were sub-standard, that there was poor application of the *CPIA* disclosure test, and "[j]udges expressed a lack of confidence in the prosecution's ability to manage the disclosure process."[198]

Similarly, in their 2016-2017 Annual Report, the Criminal Cases Review Commission, an independent investigatory body in the UK, determined the following:

> [a] major cause of miscarriages of justice continues to be non-disclosure, at or before trial, of material which could have been of assistance to the defence.
>
> Sometimes non-disclosure is deliberate. But all too often it is caused by a combination of the sheer volume of material to be considered, which in recent years has grown significantly, and the increasing pressure on the resource available to those whose duty it is to check it, almost invariably the police.[199]

Mark Heywood, the UK's most senior trial Crown, conceded this point. He remarked that pressure on resources had led to the appointment of disclosure officers who are unfamiliar with the investigation they are assigned to review, and resulted in a pressure to reduce, either consciously or unconsciously, the volume of what is "relevant"; a problem, he noted, for both the defence and the prosecution.[200]

---

197 Her Majesty's Crown Prosecution Service Inspectorate, *Making It Fair: The Disclosure of Unused Material in Volume Crown Court Cases* (UK: HMCPSI, July 2017), online: <http://www.justiceinspectorates.gov.uk/cjji/wp-content/uploads/sites/2/2017/07/CJJI_DSC_thm_July17_rpt.pdf>.

198 *Ibid* at 19.

199 Criminal Cases Review Commission, "Annual Report and Accounts 2016–2017," online:<https://s3-eu-west-2.amazonaws.com/ccrc-prod-storage-1jdn5d1f6iq1l/uploads/2015/01/1096_WLT_Criminal-Cases-Review-AR_WebAccessibleM-1.pdf> (the CCRC is a post appeal organisation created to review cases where a person has been convicted of an offence, and has exhausted their normal rights of appeal, but maintains that they have been wrongly convicted or incorrectly sentenced).

200 Interview of Mark Heywood, *supra* note 152.

V. National Security Privilege

A. Section 38 of the Canada Evidence Act

In Canada, the Crown may seek a judicial order to authorize the non-disclosure of material that must be produced to the defence under *Stinchcombe* for reasons of national security, national defence, international relations or other specified public interests.

Section 38 of the *CEA* is a complex scheme designed to apply flexibly to any judicial proceeding, be it civil, criminal, or administrative. It may be initiated by any justice participant who learns that they may be required to disclose or seek to call sensitive or potentially injurious information through written notice to the Attorney General of Canada (AGC).[201] Notice is intended to give the AGC the opportunity to review the material and, where feasible, enter into a disclosure agreement to prevent the need for "proceedings to come to a halt while the matter [i]s transferred to the Federal Court for a determination."[202]

If no agreement can be reached between the AGC and the parties, an application is made to the Federal Court and a specially designed judge will be assigned to the proceedings. In almost all circumstances a security cleared *amicus curiae* will be assigned to assist the court and, where so ordered, represent the interests of the respondent in closed proceedings.[203]

The AGC will then file the redacted material with the court. Depending on the volume of the material, the redaction and filing of documents may be done in waves over the course of months, if not years. What typically arises next is a labour and time intensive exchange of private and *ex parte* submissions and affidavits, followed by private and *ex parte* hearings including the cross examination of affiants.

Legal submissions will address the elements of the tripartite test developed in *Ribic*.[204] First, the Court must determine whether the information sought to be protected by the AGC is relevant to the underlying proceeding. The relevance threshold is low, and where the s. 38 application

---

201 CEA, *supra* note 18, s 38.01.

202 *Air India Vol 4*, *supra* note 9 at 182.

203 *Huang v Canada (AG)*, 2017 FC 662 at para 48 [*Huang*].

204 *Ribic*, *supra* note 97 at paras 17–21.

arises from a criminal prosecution it will mirror the test in *Stinchcombe*.[205] Second, the judge must assess whether disclosure of the relevant material would be injurious to international relations, national defence or national security, as outlined in s. 38.06 of the *CEA*. Third, if the disclosure of the information at issue would cause injury to a national interest, the judge must determine whether the public interest in disclosure is outweighed by the public interest in non-disclosure.

It is the party seeking disclosure that bears the burden of proving that the public interest requires disclosure.[206] In criminal cases, "to make a meaningful review of the information sought to be disclosed, the judge must be either informed of the intended defence or given worthwhile information in this respect."[207] These submissions may be made to the Court "without disclosing to any other party the substance or detail of the defence in the criminal proceeding."[208]

The s. 38 regime is extremely flexible: "the factors to be considered in determining whether the public interest is best served by disclosure or non-disclosure will vary from case to case. The judge must assess those factors which he or she deems necessary to find the balance between the competing public interests."[209] Further still, s. 38.06(2) provides that the Court may order the disclosure of the information subject to conditions or in any form the judge considers appropriate.

While the flexibility of the s. 38 regime and the *Ribic* test may be welcome in certain judicial proceedings, it creates uncomfortable uncertainty for CSIS. This uncertainty is further exacerbated in criminal proceedings where the right to a fair trial is constitutionally protected and may not be easily overcome by claims of national security.

That said, the AGC does hold a trump card. Following an order of the Federal Court for disclosure, s. 38.13(1) permits the AGC to personally issue a certificate barring its disclosure. The consequence of course, is that the trial judge may conclude that the issuance of a certificate renders a trial unfair by effectively reversing the Federal Court's finding that the

---

205 *Ibid* at para 44.

206 *Ibid* at para 21.

207 *Khawaja, supra* note 98 at para 35.

208 *Toronto Star v Canada*, 2007 FC 128 at paras 36–37, [2007] 4 FCR 434.

209 *Huang, supra* note 203 at para 50; *Khadr v Canada*, 2008 FC 549 at paras 36–39, 329 FTR 80.

information must be released to the accused. Section 38.14 authorizes a trial judge to "make any order that he or she considers appropriate in the circumstances to protect the right of the accused to a fair trial."[210] How exactly the trial judge can appropriately calibrate any such order is questionable without having access to the protected information or the Federal Court's classified reasons. This, noted the Air India Commission, "creates risks that the trial judge could err on the side of caution in protecting the accused's right to a fair trial and stay proceedings, when such a drastic remedy is not necessary to protect the accused's rights, given the nature of the non-disclosed evidence."[211]

B. Section 18.1 of the *CSIS Act*

A second statutory privilege applicable to security intelligence is found in s. 18.1 of the *CSIS Act*. This provision was introduced after the Supreme Court found in *Canada v Harkat*[212] that CSIS human sources did not benefit from the common law police informer privilege.[213]

Section 18.1 prohibits the disclosure of the identity of a CSIS human source or any information from which the identity of a human source could be inferred in a proceeding before a court, person or body with jurisdiction to compel the production of information. Unlike the s. 38 regime, the application of the privilege can only be challenged on two grounds: (1) that the individual is not a human source, meaning they did not provide CSIS with information in exchange for a promise of confidentiality; or (2) that the identity or the information protected by the privilege is essential to establish an accused's innocence in a criminal trial.[214] Any hearing respecting the privilege is to be held *in camera* and *ex parte*.[215] To date, there has been no recorded decision overturning the application of this privilege.

---

210 CEA, *supra* note 86, s 38.14 (it was this provision that was found to safeguard an accused's fair trial rights in *R v Ahmad*, 2011 SCC 6, [2011] 1 SCR 110, where the Supreme Court upheld the constitutionality of the section 38 regime).

211 *Air India Vol 4*, *supra* note 9 at 198.

212 *Canada (Citizenship and Immigration) v Harkat*, 2014 SCC 37, [2014] 2 SCR 33.

213 *Ibid* at para 87.

214 CSIS Act, *supra* note 47, s 18.1(4) (human source is defined in section 2).

215 *Ibid*, s 18.1(7).

C. UK Public Interest Immunity

As in Canada, litigating national security privilege in the UK is a balancing act. Unlike Canada, in criminal proceedings drawing the line between the rights of the accused and the risk to the public interest rest solely with the trial judge.

Traditionally, claims of "Crown Privilege" were not questioned by British Courts, and the executive took full advantage of the deference shown them by the Courts. This changed in 1968 when the House of Lords reversed their position in the landmark case *Conway v Rimmer*,[216] finding that the Court was the final arbiter when deciding whether the public interest necessitated the non-disclosure of relevant evidence.[217]

The right to disclosure in criminal proceedings is protected by article 6(1) of the *European Convention of Human Rights*.[218] The UK does not have its own bill of rights and has instead incorporated the *ECHR* into domestic legislation through the adoption of the *Human Rights Act 1998*.[219] Section 2 of the *Human Rights Act* states that all domestic courts must, in all cases, take into account the Convention rights. UK legislation must be interpreted in light of the Convention, and where legislation is found to be incompatible with the Convention, the Court may make a declaration of incompatibility.[220] It is also unlawful for a public authority to act in a manner incompatible with the Convention, however they are not liable if in accordance with domestic legislation the authority "could not have acted differently."[221]

---

216 *Conway v Rimmer*, [1968] UKHL 2, [1968] 2 ALL ER 304.

217 *Ibid.*

218 *European Convention on Human Rights*, *supra* note 33, art 6(1). Article 6(1) stipulates: "In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

219 *Human Rights Act 1998* (UK), c 42.

220 *Ibid*, s 4.

221 *Ibid*, s 6.

At first there was uncertainty as to whether common law claims for public interest immunity could be made in criminal prosecutions, but this was resolved through the passage of *CPIA* which gave the prosecutor the authority to make an application to withhold material on the basis of the public interest.[222]

In 2000, UK's procedure for adjudicating PII was at issue in three cases heard by the European Court of Human Rights (ECHR).[223] The Court found that disclosure of evidence is not an absolute right, and competing interests may be weighed against the rights of the accused so long as the measures taken are strictly necessary. The ECHR further stipulated that the aim of the state's nondisclosure must be legitimate, the trial judge must be capable of weighing the public's interest against those of the defendants, and the undisclosed material may not form part of the prosecution's case.[224]

Four years later, in the case of *R v H and C*, the House of Lords established the modern approach to PII in light of the European Court's jurisprudence interpreting the *CPIA*. The House confirmed that there may be instances where the test for disclosure set out in the *CPIA* is met but disclosure of the information would pose a serious risk to an important public interest.[225] In such circumstances, disclosure must be made to the furthest extent possible, and if limited disclosure may render the trial process unfair or the protected information may prove the accused's innocence, fuller disclosure must be ordered even if this might lead to a discontinuance to avoid making it.[226] At the same time, the House warned that "the trial process is not well served if the defence are permitted to make general and unspecified allegations and then seek far-reaching disclosure in the hope that material may turn up to make them good."[227]

---

222 CPIA, *supra* note 17, s 3(6).

223 *Rowe and Davis v United Kingdom*, [2000] ECHR 91; *Jasper v United Kingdom*, [2000] 30 EHRR 441; *Fitt v United Kingdom*, [2000] 30 EHRR 480.

224 Corker & Parkinson, *supra* note 120 at 136.

225 *H and C*, *supra* note 126 at para 18.

226 *Ibid* at para 36 (see also *R v Keane*, [1994] 1 WLR 746, where Lord Taylor remarked at para 751: "If the disputed material may prove the defendants innocent of avoid a miscarriage of justice, then the balance comes down resoundingly in favour of disclosing it.")

227 *Ibid*.

Before derogating from the "golden rule" of full disclosure the Court must ask a series of questions now codified in *Crown Court Disclosure Protocol*. These rules pronounce that "[i]t is clearly appropriate for PII applications to be considered by the trial judge"[228] as the facts and grounds to be established

---

[228] *Crown Court Disclosure Protocol*, *supra* note 129 at 13–14 (citing *H and C*, *supra* note 126 at para 36:

> When any issue of derogation from the golden rule of full disclosure comes before it, the court must address a series of questions:
>
> (1) What is the material which the prosecution seek to withhold? This must be considered by the court in detail.
>
> (2) Is the material such as may weaken the prosecution case or strengthen that of the defence? If No, disclosure should not be ordered. If Yes, full disclosure should (subject to (3), (4) and (5) below be ordered.
>
> (3) Is there a real risk of serious prejudice to an important public interest (and, if so, what) if full disclosure of the material is ordered? If No, full disclosure should be ordered.
>
> (4) If the answer to (2) and (3) is Yes, can the defendant's interest be protected without disclosure or disclosure be ordered to an extent or in a way which will give adequate protection to the public interest in question and also afford adequate protection to the interests of the defence? This question requires the court to consider, with specific reference to the material which the prosecution seek to withhold and the facts of the case and the defence as disclosed, whether the prosecution should formally admit what the defence seek to establish or whether disclosure short of full disclosure may be ordered. This may be done in appropriate cases by the preparation of summaries or extracts of evidence, or the provision of documents in an edited or anonymized form, provided the documents supplied are in each instance approved by the judge. In appropriate cases the appointment of special counsel may be a necessary step to ensure that the contentions of the prosecution are tested and the interests of the defendant protected (see paragraph 22 above). In cases of exceptional difficulty the court may require the appointment of special counsel to ensure a correct answer to questions (2) and (3) as well as (4).
>
> (5) Do the measures proposed in answer to (4) represent the minimum derogation necessary to protect the public interest in question? If No, the court should order such greater disclosure as will represent the minimum derogation from the golden rule of full disclosure.
>
> (6) If limited disclosure is ordered pursuant to (4) or (5), may the effect be to render the trial process, viewed as a whole, unfair to the defendant? If Yes, then fuller disclosure should be ordered even if this

or resisted by both parties must be carefully analyzed.[229] Furthermore, any decision with respect to disclosure must be continually reviewed as the proceedings develop in case the balance shifts.[230]

To assist the court in adjudicating PII claims, the House in *H and C,* endorsed the appointment of Special Advocates but found that "such an appointment will always be exceptional, never automatic; a course of last and never first resort."[231] Instead, the decision emphasized the need to "involve the defence to the maximum extent possible without disclosing that which the general interest requires to be protected but taking full account of the specific defence which is relied on."[232] In practice the Courts have heeded this warning. Reliance on Special Advocates is rare, noted Mark Heywood, who was unaware of any ever being appointed in a criminal case.[233]

Under the PII regime, the rules and the test for protecting sensitive information is not dependent on the source of that information.

Recognized grounds of public interest immunity include: the protection of informants and human sources, sensitive investigation and surveillance techniques, observation posts, the preservation of diplomatic relations, and national security.

In every case the court considers the same series of questions set out in *H and C.* What may vary is the procedure relied on to adjudicate the PII application, but in every instance they are heard by the trial judge.

> leads or may lead the prosecution to discontinue the proceedings so as to avoid having to make disclosure.
>
> (7) If the answer to (6) when first given is No, does that remain the correct answer as the trial unfolds, evidence is adduced and the defence advanced? It is important that the answer to (6) should not be treated as a final, once-and-for-all, answer but as a provisional answer which the court must keep under review.

229 *H and C, supra* note 126, at para 35.

230 *R v Davis*, [1993] 2 ALL ER 643, [1993] 1 WLR 613 [*Davis*].

231 *Ibid* at para 22; for a full discussion on the use of Special Advocates in the UK as compared to Canada, see Daniel Alati, *Domestic Counter-Terrorism in a Global World: Post-9/11 Institutional Structures and Cultures in Canada and the United Kingdom* (London, UK: Routledge, 2017).

232 *Davis*, *supra* note 230 at para 37.

233 Interview of Mark Heywood, *supra* note 152.

The *Criminal Rules of Procedure 2015*, sets out three forms of PII applications. The first and most common PII application is made with notice to the defence about the nature of the sensitive material, and both sides are entitled to make representations.[234] In rarer instances, the defence is not notified of the nature of the material in the application and substantive arguments are made *ex parte* (although the defence may make representations regarding procedure).[235] The final form of application is reserved for "highly exceptional" circumstances where the public interest necessitates that it be made without notice to the defence.[236]

While all forms of PII applications have been upheld by the ECHR, the Court relied heavily on the role of the trial judge and their duty to ensure trial fairness to find the second form compatible with art. 6 of the Convention.[237] As for the third type of application, the European Court strongly implied that the appointment of a Special Advocate was the only way to protect the art. 6 rights of the accused in such circumstances.[238]

1. National Security Claims for Immunity

The *CPS Disclosure Manual* specifies that the issuance of a Ministerial Certificate is the preferred means of protecting national security information. These certificates are sought when material belonging to MI5, MI6 and GCHQ "is relevant to the case, satisfies the disclosure test, if disclosed, would cause a real risk of serious prejudice to an important public interest and, the relevant agency's Minister believes properly ought to be withheld."[239]

Commonly, it will be the prosecutor, being familiar with the issues and having already seen the relevant investigative holdings, who will advise the agency that certain materials satisfy the disclosure test.[240] The agency's legal adviser will then seek instructions from their client as to whether disclosure of the identified material would cause a real risk of serious prejudice to an

---

234 *Criminal Procedure Rules*, *supra* note 167, r 15.3.

235 *Ibid.*

236 *Ibid.*

237 Dennis, *supra* note 170 at 387.

238 *Ibid* at 388 (citing *Edwards and Lewis v United Kingdoms* (2005), 40 EHRR 24, [2003] Crim LR 891).

239 *CPS Disclosure Manual*, *supra* note 141 at para 34.4.

240 *Ibid* at para 34.7.

important public interest.[241] The agency will be anxious to avoid putting unnecessary claims before the Minister,[242] who must personally review the material or a representative sample of the material before issuing a certificate.[243] Once a certificate is signed by a Minister, the Attorney General should be consulted.[244]

Unlike the Canadian s.38 regime, it is the prosecutor, not the legal advisor for the agency or the AGC who argues the PII application; it is accepted that they are in the best position to assist the court in determining where the balance between the interests lies.[245]

Although a Minister's Certificate carries considerable weight, recent case law shows that its issuance is not conclusive, and there must be evidence to support the risk asserted by the Minister.[246] Once it is established that there would be a significantly grave threat to national security, the inquiry will typically end there, however if the evidence is not dispositive the court may engage in the balancing of interests.[247] Ultimately, if the court determines that "the defendant cannot have a fair trial, there is no balance to be had."[248]

In practice, PII applications are rare. One prosecutor interview stated that she had only been involved in two in her five years with CPS, and none in the two years since she joined the Counter Terrorism Division. The Division head, Mari Read, who has been prosecuting terrorism cases since 2006 could not recall more than two cases where a PII application was necessary.

This, it was explained, is because the Crown has control of the case and the charge at a very early stage. Avoiding the need to assert privilege is the goal from the beginning, stated one CPS lawyer:

---

241 *Ibid* at para 34.11.

242 *Ibid*.

243 *Ibid* at para 34.16.

244 *Ibid* at para 34.19.

245 *Ibid* at para 34.21.

246 *Secretary of State for Foreign and Commonwealth Affairs v Assistant Deputy Coroner for Inner North London*, [2013] EWHC 3724 at paras 53–58; see also *R (Binyam Mohammed) v Secretary of State for Foreign and Commonwealth Affairs*, [2010] EWCA Civ 65.

247 *Ibid*.

248 Interview of Louis Mably, *supra* note 155.

> particularly if you are aware of issues, you don't charge where you have to disclose something. You find a way to charge something else…you find another solution. You avoid the problem in the first place. That's always the best way forward. You don't want to get yourself to a point where the decision is out of your hands. The problem with PII is the decision is out of your hands. It's up to the judge and if the judge rules against you, you've then got to drop the case. You've got to avoid getting to that place in the first place. If you do a lot of PII you're going [about it] wrong because you have not figured out what the problems and issues are early enough.[249]

Another lawyer with CPS explained that successful terrorism prosecutions are "all about strategy and working [disclosure] out beforehand… to the extent that we can front load it."

Thus it is the *CPIA* disclosure regime, and not the method for adjudicating privilege that is fundamental to the protection of national security information in the UK. "If relevance was the test of disclosure in any way" remarked Mark Heywood, "we'd have a nightmare. Relevance is elastic… it would be unending litigation."[250]

VI. FINDINGS AND RECOMMENDATIONS

A. Findings

The application of the Canadian disclosure regime to terrorism prosecutions results in unending litigation about the provision and protection of information. This litigation is not only inefficient, it creates uncertainty for CSIS who is unable to predict whether their information will be subject to *Stinchcombe* disclosure, sought in an *O'Connor* application for third party information, or released by the Federal Court following a s. 38 application. For an organization whose mandate cannot be met without collecting secrets, working covertly, and protecting the anonymity of its sources and employees this uncertainty is a nightmare.

The UK system facilitates bringing terrorists to trial. Through interviews it became clear that the aim of the Crown Prosecution Service is not to prosecute every terrorist to the fullest extent of the law but to disrupt terrorist activity and get members and facilitators of terrorist organizations off the streets. The *CPIA* empowers the prosecution to do this by charging lesser offences and consequently disclosing less sensitive material. Secure in

---

249 Interview of Jess Hart, *supra* note 130.

250 Interview of Mark Heywood, *supra* note 152.

the knowledge that the Crown Prosecutors will set the proceedings on a course to eliminate, to the greatest extent possible, the need to disclose sensitive material, the security services and police are not hesitant to share information and work jointly on national security investigations.[251]

In Canada, however, there is no incentive to charging lesser offences when the disclosure regime necessitates the release of all relevant investigative materials, both inculpatory and exculpatory. Instead, an increasing number of alternate measures to prosecution have been introduced to disrupt terrorists, prevent them from travelling, and limit their access to resources and networks.[252]

Additionally, the *CPIA* and its corresponding regulations and guidelines promote trial efficiency by making it the duty of both the prosecution and defence to identify and narrow issues for trial and ensure that the necessary information is disclosed even where the source of that information must be protected. The effect is that all parties are responsible for working together to find the right balance between the interests of justice and the protection of national security.

Nevertheless, wholesale importation of the *CPIA* is not the answer to Canada's I2E problem. First, as discussed briefly above, recent review in the UK has identified that the police and crown routinely fail to comply with the *CPIA*, creating opportunities for the miscarriage of justice.

Second, in Canada, the right to make full answer and defence is enshrined in s. 7 of the *Charter*. In *Stinchcombe*, the Supreme Court rejected the argument that the accused's constitutional right to the disclosure is limited to exculpatory evidence. While the Court held that the right to Crown disclosure is not absolute, it "admits…few exceptions."[253] Thus, as the Air India commission identified, introducing legislation exempting injurious national security information from Crown disclosure would violate s. 7 and would have to be justified as a reasonable limit under s. 1 of the *Charter*.[254]

Third, in Canada, s. 7 protects the right against self-incrimination and the associated right to remain silent. The Supreme Court in *Stinchcombe* found that there was no corresponding duty on the defence to disclose

---

251 Evidence of Joe Fogarty, *supra* note 28.

252 *False Security*, *supra* note 7 at 282.

253 *McNeil*, *supra* note 85 at para 18.

254 *Air India Vol 4*, *supra* note 9 at 155.

material to the Crown because "the defence has no obligation to assist the prosecution and is entitled to assume a purely adversarial role toward the prosecution."[255] This is altogether different than the UK, where the *CPIA* requires active and ongoing defence participation. Prosecutors rely on defence disclosure to identify issues, defences, and potential witnesses when applying the disclosure test to unused material. There are consequences if an accused fails to cooperate with the Crown, and negative inferences may be drawn if issues or defences are not raised as soon as practicable in the proceedings. Imposing requirements of defence disclosure to this extent within the Canadian criminal justice system would certainly be vulnerable to constitutional challenge.

B. Recommendations

1. Recommendation: Codify the Definition of Relevance

While adopting the CPIA is not a viable option, nothing prevents Parliament from codifying a standard of relevance under the CEA that is commensurate with the standard set out in Stinchcombe. The common law interpretation of relevance as that which is "not clearly irrelevant" is unhelpful and provides little guidance to law enforcement, CSIS, and the Crown. It is recommended that Canada adapt and codify the UK's definition of relevance as follows:

> Material is relevant and must be disclosed to the accused if:
>
> a) it is in the possession or has been inspected by the Crown, and
> b) has some bearing on any offence charged, or on the surrounding circumstances of the Crown's investigation;
> c) unless the material satisfying a) and b) is incapable of having any impact on the case against the accused, or of assisting the case for the accused.

---

255 *Stinchcombe*, *supra* note 16 at 333.

2. Recommendation: Codify Third Party Disclosure for Terrorism Prosecutions

Parliament is also free to legislate new procedures for the production of CSIS records for terrorism proceedings. The goal of such legislation would be to limit litigation around the production of CSIS records under *O'Connor* and minimize the need to make applications for non-disclosure under the *CEA*. As noted by the Air India Commission, it would also "respond to concerns that the breadth of *Stinchcombe* and *O'Connor* may have adversely affected relations between the RCMP and CSIS and the passage of secret intelligence to the police."[256]

In *R v Mills*,[257] the Supreme Court held that it was open for Parliament to enact a statutory limit on the common law right to third party disclosure.[258] Subsequently, in *McNeil*, the Court relied on its decision in *Mills* to find that statutory exceptions to both the *Stinchcombe* and *O'Connor* disclosure regime may be "nonetheless constitutional."[259]

As discussed in Part IV, *Stinchcombe* disclosure is premised on two assumptions, that material in the possession of the Crown is relevant to the accused's case (otherwise it would not be in the possession of the Crown) and that this material will comprise that case against the accused. Terrorism proceedings result in three additional assumptions: (1) CSIS will have records pertaining to the accused's terrorist activities, and (2) these records will not comprise the criminal case against the accused; and (3) these records will likely consist of highly sensitive material that is not relevant to issues at trial.[260]

In recognition of this first assumption, a third party regime for terrorism proceedings should impose a duty on the Crown to make inquiries with CSIS when prosecuting terrorism offences. Identified records should be reviewed and assessed by the Crown Prosecutor for their "likely relevance." If there is a "reasonable possibility that the information is logically probative

---

256 *Air India Vol 4*, *supra* note 9 at 158 (the Commission suggested that the modification of the third party disclosure similar to the regime limiting access to records of sexual assault victims under the *Criminal Code* may provide a more nuanced solution to reform to Crown Disclosure under *Stinchcombe*, at 156).

257 *R v Mills*, [1999] 3 SCR 668, 1999 CanLII 637 [*Mills*].

258 *Ibid*.

259 *McNeil*, *supra* note 85 at para 21.

260 Cohen, *supra* note 113 and accompanying text.

to an issue at trial or the competence of a witness to testify" the information is disclosable to the defence.[261]

Such a duty would be compatible with the Crown's role as a Minister of Justice and their undivided loyalty to the proper administration of justice.[262] In *McNeil,* the Supreme Court affirmed that "Crown Counsel have a duty to make reasonable inquiries of other Crown agencies or departments that could reasonably be considered to be in the possession of evidence."[263] The Court recognized that as both an advocate and an officer of the Court, "Crown counsel can effectively bridge much of the gap between first party disclosure and third party production."[264]

The second assumption necessitates limited participation by the defence to identify potential issues for trial that the Crown must consider when reviewing CSIS documents. The Crown and the defence must then make a good faith effort to identify pertinent records. Imposing a significant but not onerous burden on the defence is consistent with their obligation under *O'Connor* to satisfy the court through a particularized request that third party documents exist and how they could assist the defence.[265] It is also consistent with the recognized need to prevent the defence from engaging in "fishing expeditions"[266] for irrelevant evidence at the expense of the effective administration of justice.[267]

While it may be argued that obligating even limited defence disclosure is a violation of an accused's s. 7 rights, the Supreme Court in *R v MPB*,[268] remarked that the protection against disclosure is not an absolute right.[269]

---

261 *McNeil*, *supra* note 85 at para 33 [emphasis added].

262 *Ibid* at para 49.

263 *Ibid* at para 49 (citing *R v Arsenault* (1994), 153 NBR (2d) 81 at para 15 (CA)).

264 *McNeil*, *supra* note 85 at para 51.

265 The role of the defence was fully canvassed in the Lesage-Code Report who provided a series of recommendations for third-party disclosure requests in complex trials. See Patrick Lesage & Michael Code, *Report of the Review of Large and Complex Criminal Case Procedures* (Toronto: Ontario Ministry of the Attorney General, 2008) at 45-55 [*LeSage-Code Report*].

266 *Ibid* at 48.

267 *Ibid* at 47–48.

268 *R v P (MB)*, [1994] 1 SCR 555, 1994 CanLII 125.

269 *Ibid*; *R v Chaplin*, [1995] 1 SCR 727, 96 CCC (3d) 225 at 227–228, 237 (Justice Sopinka upheld the policy purpose for placing the onus on the defence "to preclude speculative, fanciful, disruptive, unmeritorious, obstructive and time consuming disclosure requests

It is also questionable whether identifying possible defences and deficiencies in the Crown's case is truly assisting the prosecution.

Respecting the third assumption, once the Crown identifies disclosable information in the Service's possession, they must engage with the Service to determine the most appropriate way to provide that information to the accused in light of any applicable privileges. As in the UK, the common law does not require the disclosure of original third party records; the test in *O'Connor* speaks only to the production of likely relevant *information.*[270] This disclosure obligation could be met in various ways: redacting documents, providing summaries, admitting facts, drafting witness statements, etc. Depending on the mechanism selected, it may result in the "Crown holding documents that the accused does not possess";[271] however this, the Supreme Court found in *Mills*, "does not of itself deprive the accused of the right to make full answer and defence."[272]

As Justices LeSage and Code noted in their 2008 report of their review of complex mega-trials:

> If both counsel remember their duties as "officers of the court" and as "ministers of justice", then it should only be in an exceptional case that disclosure requests need to be the subject of a motion in court. Most disclosure disputes are amenable to reasonable compromise and counsel on both sides have a duty to seek such compromises.[273]

In circumstances where likely relevant Service information cannot be produced because its disclosure in any form could injure international relations, national defence or national security, or violate human source privilege under s.18.1 of the *CSIS Act*, notice would then be given to the AGC. If the AGC does not permit the disclosure of the likely relevant material, an application to withhold the information should be made to the trial judge and argued *in camera* and *ex parte* by the Crown and Counsel for the AGC. *Amici curiae* could be appointed to assist the trial judge, and where so ordered represent the interests of the accused in the *ex parte* proceedings.

... Fishing expeditions and conjecture must be separated from legitimate requests for disclosure").

270 *O'Connor, supra* note 89 at para 19.

271 *Mills*, *supra* note 253 at para 116.

272 *Ibid.*

273 *LeSage-Code Report*, *supra* note 265 at 49.

It is not recommended that the adjudication of national security claims before the trial judge replicate the s. 38 *CEA* process. The application of the *Ribic* test requires the balancing of the national security interest in protecting the information against the public interest in its disclosure. The test does not only require the production of information where the accused's innocence is at stake or where trial fairness is at risk: any arguable interest may be sufficient to merit the release of documents if a judge deems that it outweighs the national security risk. Further still, a judge need not accept the Attorney General's assessment of the risk or injury that would arise if material were disclosed, and may call for its release even where the accused's interests are not at stake so long as the material is relevant under *Stinchcombe*. Thus, the *Ribic* test, while flexible, is unpredictable and its litigation is long and complex.

For this reason, this author suggests that when determining whether to order the disclosure of sensitive CSIS records that the Crown has identified as likely relevant in a terrorism proceeding, the court should be limited to two discrete questions. First, would the release of the information at issue cause injury to national security? If the answer is no then the information must be disclosed. Second, if the injury is made out, is disclosing the information essential to trial fairness? If trial fairness necessitates the information's disclosure, the Crown and the AG would have two options: disclose the material or stay the proceedings.

Having seen the Service's holdings, the Crown Prosecutor could re-visit disclosure decisions throughout the proceedings if an issue arises that changes the likely relevance of CSIS material. The Court would also be in a position to reassess their findings regarding trial fairness as evidence is presented. However, no appeal of a disclosure decision should be permitted until the conclusion of a trial resulting in a conviction.

3. Recommendation: Specialized Crowns and Judges

To make this regime work, Canada should look to the UK as a model and establish a division of specialized terrorism prosecutors within the Public Prosecution Service. Not only would terrorism counsel need to have the necessary security clearance to review Service documents, but it would also be essential for them to gain experience and an understanding of CSIS operations and reporting, and build trust with CSIS officials. Having dedicated counsel assigned to terrorism prosecutions would also facilitate earlier consultation regarding the impact of intelligence sharing between

CSIS and the RCMP, and the implications for charging and disclosure. It would also be advantageous to have dedicated Superior Court Judges in each jurisdiction assigned to case manage and preside over terrorism prosecutions as soon as initial pre-trial custody hearings are complete.

4. Recommendation: Codify Witness Anonymity and Protection

Finally, it is recommended that s. 486 of the *Criminal Code* be amended to enhance the protection of witnesses in terrorism prosecutions. In the UK, MI5 has become less reluctant to have their employees testifying in criminal proceedings because there is certainty and an understanding of how their identity will be protected.[274] The *Criminal Code* should be amended to provide for the testimony of witnesses in terrorism trials under a pseudonym, and also permit their voice and image to be obscured where the Crown can establish that such measures are necessary in the interest of justice.[275] The entrance and exit of such a witnesses into the courtroom should also be made via a closed route, and applications for the adoption of such measures should be heard *in camera*, and where necessary *ex parte*.

VII. CONCLUSION

There is no disputing that Canada has an intelligence to evidence problem. Since the establishment of CSIS, the Crown's obligation to disclose all material in its possession that is not clearly irrelevant has made the Service apprehensive about sharing its intelligence with the RCMP. This apprehension is exacerbated further by the uncertainty built into the s. 38 *Ribic* test and the Federal Court's balancing of interests. Add to this, the possibility that CSIS records, never revealed to law enforcement, may be ordered disclosed on the basis that they are "likely relevant" creates an untenable level of risk for an organization preoccupied with protecting the secrecy of its partners, sources, techniques and employees. Thus, to avoid the hazards tied to criminal disclosure obligations, CSIS and the RCMP engage in parallel investigations, and Crown Prosecutors are unable to

---

274 Interview of Mari Reid, *supra* note 123.

275 See Security Service "Evidence and Disclosure," online: <https://www.mi5.gov.uk/evidence-and-disclosure>; UK AG's Legal Guidance on "Witness Protection and anonymity," online: <http://www.cps.gov.uk/legal/v_to_z/witness_protection_and_anonymity/#a06>.

leverage the information in the possession of Canada's national security agencies to bring terrorists to justice.

The UK does not struggle with the same dilemma. Interviews undertaken for this article reinforced the importance of clear guidelines for the disclosure of Crown material and third party production. Legislating similar guidelines for CSIS records that respect the fundamental principles of justice protected by s. 7 of the *Charter* will provide greater certainty to the Service when making choices about what and how much information to share with the RCMP.

The reforms suggested in this article are also likely to incentivize the Service, the Crown and the defence to work together to find a means of disclosing the necessary information while protecting the source of that information. Certainty would also be enhanced by limiting the discretion of the Court. Should disclosable information be too sensitive to release in any form, the question of whether it should be disclosed should not be left to a judge to balance against the interests of the accused. The test for disclosure in such circumstances must be discreet: if the information would be injurious to national security it cannot be released. Once the injury is made out, the level of risk to Canada's national security should not be left to a judge to adjudicate. Instead, the trial judge should assess whether withholding the information would render the trial unfair or place the innocence of the accused at stake. If the judge finds that a trial cannot proceed fairly without the disclosure of the sensitive information, the state is left with a policy choice: release the information or withdraw the prosecution. Either option creates a risk to national security, one that only the Government of Canada is competent to make.