advocates in public interest immunity proceedings, while also indicating some awareness that delay may be caused as the special advocate becomes familiar with the case and that ethical problems may emerge from restrictions on the special advocate in communicating with the accused after the special advocate has seen the secret information. Both the United States and Australia provide for the alternative of defence counsel themselves being able to examine the sensitive material contingent on obtaining a security clearance. Although the process of obtaining a security clearance could cause delay and adversely affect choice of counsel, it also allows the person most familiar with the accused's case to have access to secret material in order to make arguments about whether its disclosure is necessary for a fair trial. Security clearance requirements may also encourage the use of experienced defence lawyers in terrorism trials. The Australian experience also suggests that the creative use of testimony by closed-circuit television can help in reconciling competing interests in disclosure and fairness when members of foreign or domestic intelligence agencies testify in terrorism prosecutions.

Conclusions

A) The Evolving Relation Between Intelligence and Evidence

What might be seen as intelligence at one point in time, might be evidence at another point in time.[669] There is a need to re-examine traditional distinctions between intelligence and evidence in light of the particular threat and nature of terrorism and the expanded range of crime associated with terrorism. Terrorism constitutes both a threat to national security and a crime. Although espionage and treason are also crimes, the murder of civilians in acts of terrorism such as the bombing of Air India Flight 182 demands denunciation and punishment that can only be provided by the criminal law. The same is true with respect to intentional acts of planning and preparation to commit terrorist violence. Although attempts and conspiracies to commit terrorist violence have always been serious crimes, the 2001 *Anti-Terrorism Act* has changed the balance between intelligence and law enforcement matters by creating a wide range of terrorist offences that can be committed by acts of preparation and support for terrorism which will occur long before actual acts of terrorism. The prevention of terrorism must remain the first priority, but

669 Fred Manget "Intelligence and the Criminal Law System" (2006) 17 Stanford Law and Public Policy Review 415 at 421-422.

wherever possible, those who plan, prepare or commit acts of terrorism should be prosecuted and punished. Both Canada's domestic laws and its international obligations demand the prosecution and punishment of terrorism.

There is some concern that CSIS continues to resist the need to gather information in counter-terrorism investigations to evidentiary standards. In contrast, MI5 has the disclosure of information relating to the prevention of serious crime and for criminal proceedings as part of its statutory mandate and it has stated that it will gather some evidence relating to surveillance to evidential standards. With respect to Air India, CSIS information in the form of wiretaps and witness interviews could have been some of the most important evidence in the case, but, unfortunately, they were destroyed in part because of CSIS's understanding of its role as a security intelligence agency that does not collect or retain evidence. The failure to retain and disclose such material can harm both the state's interests and those of the accused.

Although CSIS is not mandated to be a law enforcement agency, s.19(2)(a) of the *CSIS Act* contemplates that it will collect information that will have significance for police and prosecutors for investigations and prosecutions and that it may disclose such information to police and prosecutors. There has never been a statutory wall between intelligence and evidence or between CSIS and the police in Canada. Section 18(2) of the *CSIS Act* also contemplates that the identity of confidential sources and covert agents may also be disclosed as required in criminal investigations and prosecutions. Section 12 of the *CSIS Act* should not be taken as authorization for the destruction of information that was collected in accordance with its requirement that information only be collected to the extent that it is strictly necessary. Stark contrasts between the reactive role of the police in collecting evidence and the proactive role of CSIS in collecting intelligence drawn by the Pitfield committee and others have not been helpful. The *CSIS Act* never contemplated an impenetrable wall between intelligence and law enforcement. Although this should have been clear in 1984, it should have been beyond doubt after the Air India bombing, let alone 9/11.

B) The Case Studies: Canada's Difficult Experience with Terrorism Prosecutions

The case studies examined in this study raise doubts about whether Canadian practices and laws are up to the demands of terrorism prosecutions, particularly as they relate to the relation between intelligence and evidence and the protection of informants. The Parmar prosecution in Hamilton, the Khela prosecution in Montreal and the Atwal prosecution in British Columbia all collapsed because of difficulties stemming from the requirements that the state make full disclosure of relevant information including the identity of confidential informants. The disclosure of the affidavit used to obtain the CSIS wiretap in Atwal disclosed inaccuracies and led to the resignation of the first director of CSIS. The disclosure of the affidavit in the Parmar prosecution also revealed inaccuracies that would have allowed the defence lawyers to cross-examine those who signed the affidavit. Both the Parmar and Atwal cases involved the then novel procedure of giving the accused access to affidavits used to obtain wiretaps and it is hoped that wiretap practice has improved and adjusted to the demands of disclosure. There is an ability to edit affidavits to protect public interests in non-disclosure, but the information that is edited-out cannot be used to support the validity of the warrant. Similarly, witness protection programs have become more formalized and may have improved since the Parmar and Khela prosecutions collapsed in part because of a reluctance of informers to have their identities disclosed to the accused because of fears for their safety. Nevertheless, these cases underline the likelihood of disclosure when judged necessary for the accused to make full answer and defence and the importance of protecting informers when intelligence is used as evidence in terrorism prosecutions.

The Kevork and Khawaja terrorism prosecutions, as well as the Ribic hostage- taking prosecution, all demonstrate a different type of problem. They were all delayed and disrupted by separate national security confidentiality proceedings in the Federal Court. Section 38 places strains on the prosecution process because it requires the Federal Court to make decisions about non-disclosure without having heard the evidence in the criminal case. In turn, it places strains on a criminal trial judge who is in the difficult, if not impossible, position of deciding whether non or partial disclosure with respect to information that the accused and even the trial judge have not seen will nevertheless adversely affect the accused's right to a fair trial and full answer and defence.

The awkward s.38 procedure was only avoided in the Malik and Bagri prosecution because the experienced counsel on both sides were able to agree on an innovative approach that included inspection of CSIS material by the defence on initial undertakings that it not be shared with their clients. Without this procedure, one that may not be easily duplicated and could require defence lawyers to obtain security clearances, the Malik and Bagri prosecution could easily have been further delayed and perhaps even halted because of the litigation of s.38 issues. A stay of proceedings or another remedy might also have been entered as a response to CSIS's destruction of tapes and witness statements had the trial judge not decided to acquit the accused. In some respects, it was a minor miracle that the case reached verdict.

Attempts have been made to encourage pre-trial resolution of s.38 issues, but the *Ribic* case and the reality of late disclosure in complex cases including the *Khawaja* prosecution suggest that a terrorism prosecution could be beset by multiple s.38 applications and by multiple trips to the Federal Court and appeals to resolve these issues. The United Kingdom and the United States have much more experience with terrorism prosecutions than does Canada and it is noteworthy that they allow the trial judge to make non-disclosure decisions on the grounds of national security confidentiality. This allows such issues to be integrated into overall trial-management issues and it allows the trial judge to revisit an initial non-disclosure issue should the evolving issues at trial suggest that fairness to the accused requires disclosure. At this point, the prosecution may face the difficult choice of whether to disclose the secret information or to halt the prosecution through a dismissal of charges or a stay of proceedings. This difficult decision, however, will not be made prematurely. It will only have to be made after a fully informed trial judge has decided that disclosure is necessary to ensure fairness towards the accused.

C) Front and Back-End Strategies for Achieving a Workable Relation Between Intelligence and Evidence

Intelligence can be protected from disclosure by not bringing prosecutions or by halting prosecutions, including through a non-disclosure order issued by the Attorney General of Canada under s.38.13 of the CEA. Nevertheless, such non-prosecution strategies are not attractive in the face of deadly terrorist plots that require prosecution and punishment. Leaving aside non-prosecution, there are two broad strategies available

to deal with the challenges presented by the need to establish a workable relation between intelligence and evidence.

One broad strategy is front-end and involves changing the nature of secret intelligence to make it usable in criminal prosecutions. These changes would be directed at the practices of CSIS to ensure that where possible they collect intelligence to evidential standards in counter-terrorism investigations and that they consider source and witness protection should it become necessary to disclose the identity of confidential informants. It will also require co-operation between CSIS and the RCMP and other police forces involved in terrorism prosecutions so that Criminal Code procedures, especially with respect to wiretaps, are used when appropriate. The challenges of these front-end reforms, especially to CSIS and to foreign agencies that share information with Canada subject to caveats that the information not be disclosed, should not be underestimated.

The second strategy focuses on the back-end procedures that can be used in court to reconcile the need to keep secrets with the need to disclose material. They involve the rules governing disclosure and production obligations and evidentiary privileges. These reforms are designed to shield intelligence and other material from disclosure in all cases. Such strategies may attract Charter challenges by limiting disclosure obligations across the board and they risk being held to be over-broad in a particular case. Fortunately, back-end strategies include better-tailored procedures to adjudicate claims of national security confidentiality on the facts of specific cases. It will be suggested that this process can be made more efficient and more fair by focusing on the concrete and specific harms of disclosure of secret information and by allowing trial judges to make, and when necessary to revise, non or modified disclosure decisions.

D) Front-End Strategies to Make Intelligence Useable in Terrorism Prosecutions

1. Collection and Retention of Intelligence With Regard to Evidential and Disclosure Standards

One important front-end strategy is for security intelligence agencies to have more regard for evidentiary and disclosure standards when they collect intelligence in counter-terrorism investigations. The likelihood of prosecution and the possible disclosure or use of some forms of

intelligence as evidence has increased since CSIS was created in 1984. This is because the threat of terrorism has increased, disclosure and production standards have increased and many new crimes with respect to the support and financing of terrorism and preparation for terrorism have been created. It will be a rare counter-terrorism investigation where there is not some possibility of a crime being committed and a prosecution being appropriate. This may not necessarily be the case with counter-intelligence or counter-espionage investigations.

In some cases, intelligence agencies such as MI5 and ASIO consciously collect evidence to evidentiary standards in the expectation that their agents may be required to produce such material to the prosecution and to testify in court. The Malik and Bagri prosecutions, however, reveal that CSIS agents at that time did not collect or retain the fruits of their terrorism investigations to evidentiary standards or with a view to a prosecution. Although the acquittal avoided the need to fashion a remedy, the trial judge found that CSIS's failure to retain relevant material including not only the wiretaps but also notes of an interview with a key witness violated Malik and Bagri's rights under s.7 of the Charter. In terrorism investigations, CSIS and other intelligence agencies should constantly evaluate the likelihood of a subsequent prosecution and the effect that a prosecution could have on secret intelligence. Where possible, they should collect and retain information to evidentiary standards.

Section 12 of the CSIS Act should not have prevented the retention of properly obtained information, but some clarification of s.12 is desirable to make clear that CSIS should retain properly obtained information when it may become relevant to criminal investigations and prosecutions. One option would be to abandon the requirement in s.12 that information and intelligence be collected with respect to activities that on reasonable grounds are suspected of constituting threats to the security of Canada only "to the extent that it is strictly necessary". Such an approach, however, would sacrifice values of restraint and privacy that are protected by the "strictly necessary" standard. A better approach is to make clear that if information is properly collected under the "strictly necessary" standard, it should be retained when it might be relevant to the investigation and prosecution of a criminal offence that also constitutes a threat to the security of Canada. Another option would be to require the retention of information that may be relevant to the investigation or prosecution of a terrorism offence as defined in s.2 of the Criminal Code.

Privacy concerns raised by any increased retention of information can be satisfied by adequate review of the legality of its collection, including the requirement that the collection be "strictly necessary" to investigate activities that may on reasonable grounds be suspected of being threats to the security of Canada. The Inspector General of CSIS, the Security Intelligence Review Committee and the Privacy Commissioner can all review not only the collection of the information but the manner in which it is retained and the manner in which is distributed to other agencies.

Information obtained under a warrant issued under s.21 of the CSIS Act could also be retained at least for the duration of the warrant albeit with restrictions on who has access to the information and with review of any information sharing. There may be a case for judicial authorization and control of information collected under a s.21 wiretap warrant. Retained intelligence should be distributed when required for a criminal investigation or prosecution as contemplated under s.19(2)(a) of the CSIS Act. There may be a case for amending s.19(2) (a) to require CSIS to disclose information that may be used in a criminal investigation or prosecution to the police and to the relevant Attorney General. The idea that CSIS could exercise their present residual discretion to refuse to disclose such information in order to protect the information from disclosure is problematic. There is a danger that acts of terrorism that could have been prevented by arrests or other law enforcement activity will not be prevented if the information is not passed on to the police. Even a refusal to pass on the information does not guarantee that an accused will not seek disclosure or production if the information becomes truly relevant to a subsequent criminal prosecution. If CSIS does pass on the information, the Attorney General of Canada would still retain the option of seeking a non-disclosure order for the secret information or issuing a non-disclosure certificate under s.38 of the CEA in order to prevent the harms of disclosure.

Although the Air India investigation had unique features that led to CSIS being held to be subject to disclosure and retention of evidence obligations under *Stinchcombe,* it would be a mistake for CSIS to conclude that the fruits of its counter-terrorism investigations could be absolutely protected from disclosure or that CSIS has a discretionary veto on disclosure requirements. Even if CSIS is considered to be a third party for purposes of disclosure, the accused in a terrorism trial may be able to make demands for disclosure of some CSIS material. The courts will impose a slightly higher standard on the accused to obtain production

from CSIS as a third party under *O' Connor* than as part of the Crown under *Stinchcombe*, but the courts will still require production when it is required to ensure fairness to the accused.

Some changes in the organizational culture of Canada's security intelligence agencies may be required to deal with the challenges of terrorism prosecutions. The need to protect secrets takes on a new dimension when the targets of intelligence are about to blow airplanes out of the sky. Intelligence agencies must adapt to the new threat environment and the increased possibility that their counter-terrorism investigations may reach a point where it is imperative that the police arrest and prosecute people. Security intelligence agencies must resist the temptation to engage in over-classification and unnecessary claims of secrecy. It is not good enough for security intelligence agencies which are increasingly focusing on counter-terrorism to rely on old mantras that they do not collect evidence.

Security intelligence agencies need to adjust their approaches to disclosure and secrecy to take into account that terrorism is now considered to be the greatest threat to national security and that they will often work along side the police in trying to prevent terrorist violence. Mechanical and broad approaches to secrecy may have been appropriate during the Cold War when the greatest threat to national security came from Soviet spies, but they are not appropriate in counter-terrorism investigations where the prospect of arrest and prosecution looms large. Starting with the Air India investigation and the *Atwal* case, CSIS has not had a happy experience with disclosure of information to the courts and it must put this unhappy experience behind it. Because of Canada's status as a net importer of intelligence, there may be tendency to err on the side of secrecy over disclosure. Nevertheless, the courts have since *Atwal* placed demands on CSIS for disclosure. More recently, courts are re-examining Cold War concepts such as the fear that a hostile state will piece together various bits of innocuous information through the mosaic effect. They are also recognizing that Canada can ask its allies under the third party rule to consent to the disclosure of intelligence and that the third party rule does not apply to information that is already in the public domain.[670] All of these changes point in the direction of the increased disclosure of intelligence in the future.

---

670 *Canada v. Commission of Inquiry* 2007 FC 766; *Canada v. Khawaja* 2007 FC 490.

Evidentiary standards and disclosure to the court and to the accused, however, will not be possible in all cases. Security intelligence agencies must respect their statutory mandate which is to provide secret intelligence to warn the government about security threats and not to collect evidence. In addition, they must also respect restrictions on the use of intelligence that is provided by foreign agencies and they must protect their confidential informers and their agents. The protection of such information will require back-end strategies to ensure non-disclosure. More effort needs to be made by security intelligence agencies to understand the ability of the legal system to protect secrets from disclosure and to educate other actors and the public about the legitimate needs for secrecy. Justice O'Connor has warned that overclaiming of national security confidentiality could create public suspicion and cynicism about secrecy claims.[671] There needs to be better understanding about the legitimate need to keep secrets with respect to intelligence from our allies, ongoing investigations, secret methods and vulnerable informants.

2. Seeking Amendments of Caveats under the Third Party Rule

Canada's status as a net importer of intelligence will continue to present challenges for the management of the relation between intelligence and evidence. Canada must encourage foreign governments to share intelligence with Canada and it must respect caveats or restrictions that foreign states place on intelligence that they share with Canada. That said, the third party rule that honours caveats is not an absolute and static barrier to disclosure when required for terrorism prosecutions. The third party rule simply prohibits the use and disclosure of intelligence without the consent of the agency that originally provided the information.

A front-end strategy that can respond to the harmful effects of caveats on terrorism prosecutions is to work with foreign partners to obtain amendments to caveats that restrict the disclosure of information for purposes of prosecution. Much intelligence that the police receive from foreign and domestic intelligence agencies contains caveats that restrict the subsequent use of that intelligence in prosecutions. The Arar Commission has recently affirmed the importance of such caveats, as

671 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Public Works and Government Services) at pp 302, 304

well as the need to ensure that intelligence is accurate and reliable. At the same time, it also made clear that amendments to caveats can be sought and obtained in appropriate cases.[672] The recent decision in *R. v. Khawaja*[673] has indicated that the third party rule should not be applied in a mechanical fashion to prevent disclosure of information that was already possessed by Canada or was in the public domain. Even when the third party rule applies, Canada should request permission from foreign agencies to allow the disclosure of information for the limited purposes of terrorism prosecutions. The idea that relationships with foreign agencies or that Canada's commitment to the third party rule will be shaken by even requesting amendments to caveats should be rejected. Foreign agencies who are also facing demands for disclosure in terrorism prosecutions in their own countries, should understand that a request to amend the caveats that they placed on information demonstrates respect for the caveat process. In some cases, foreign agencies may consent to the disclosure or partial disclosure of intelligence. The time lag between the initial collection of intelligence and its possible disclosure in a subsequent terrorism prosecution may allow caveats to be lifted or amended. In other cases, the foreign agencies will refuse to amend caveats that restrict the subsequent disclosure of information. In such cases, Canada has the tools necessary, including the use of a certificate under s.38.13 of the CEA, to honour its commitments to allies.

3. Greater Use of Criminal Code Wiretap Warrants

Another front-end strategy is to make greater use of Criminal Code authorizations for electronic surveillance in terrorism investigations where prosecutions are expected. The use of such warrants would avoid the questions of whether electronic surveillance conducted by CSIS, the CSE or foreign intelligence agencies would be admissible in Canadian criminal trials. The ATA has made it easier to obtain Criminal Code electronic surveillance warrants in terrorism investigations by eliminating a requirement to establish investigative necessity and extending the duration and notification requirements of the warrants. Such a strategy will, however, require close co-operation between CSIS and the police and a willingness to allow the police to take the lead in a terrorism investigation where grounds exist for obtaining a Criminal Code wiretap warrant.

---

672 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar Analysis and Recommendations* (Ottawa: Government Services, 2006) at 318-322, 331-332.

673 2007 FC 490 rev'd on other grounds 2007 FCA 342.

Criminal Code authorizations present their own challenges relating to the need to disclose much of the information used to obtain the judicial authorization, but the rules relating to disclosure and admissibility are clearer than with respect to security intelligence. The Part VI scheme has been upheld as constitutional by the Supreme Court and the rules and procedures for editing the affidavit to protect public interests in non-disclosure are clear. The same cannot be said about the scheme for CSIS wiretaps which were held to be constitutional in a divided decision by the Federal Court of Appeal twenty years ago.[674] That said, the grounds for editing the affidavit used to obtain a wiretap warrant under s.187(4) of the Criminal Code could perhaps be expanded to allow the deletion of material that would reveal and prejudice intelligence gathering techniques even if disclosure would not endanger the persons engaged in those techniques. Other Criminal Code warrants may also be used in terrorism investigations and judges can order that information relating to such warrants not be disclosed for various reasons listed under s.487.3 of the Criminal Code. These grounds are open-ended and include protection for confidential informants and ongoing investigations, but could be expanded to include the need to protect intelligence gathering techniques. State interests in secrecy will have to be reconciled with competing concerns about open courts and fairness to the accused in the particular circumstances of each case. Criminal Code warrant procedures provide an established and constitutional basis for the reconciliation of the competing interests. Material that is edited out of the affidavit used to obtain the warrant and not disclosed to the accused cannot generally be used to sustain the warrant. As will be suggested below, security cleared special advocates could be given access to the unedited affidavit and other relevant material in order to represent the accused's interests in challenging both Criminal Code and CSIS warrants. Such an approach could help protect intelligence and other sensitive material from disclosure to the accused while allowing it to be subject to adversarial challenge.

In appropriate cases the state should continue, as it did in the *Atwal* case, to argue for the admissibility of security intelligence intercepts in criminal trials. These arguments will have a better chance of success in cases where the intelligence was gathered as a part of the intelligence mandate and "the Rubicon" had not been crossed into law enforcement activity. Although Criminal Code authorizations may be possible and helpful in some cases,

---

674 *R. v. Atwal* (1987) 36 C.C.C.(3d) 161 (Fed.C.A.).

intelligence agencies still have an important regulatory mandate to collect intelligence through their own special standards. In appropriate cases, intelligence intercepts could be admitted as evidence in criminal trials on the basis that the law authorizing the search is reasonable or that any departure from regular criminal law standards can be justified under s.1 of the Charter given the primary objective of collecting information to inform the government of threats to the security of Canada.

It may also be advisable to amend s.21 of the CSIS Act to make clear that a warrant can be issued to CSIS to conduct electronic surveillance outside Canada. It may be preferable to have CSIS conduct such operations with the consent of the foreign country than to rely on the foreign agencies to conduct such surveillance. The activities of the foreign agency will not be bound by the Charter and they may not have the same priorities or procedures as CSIS. An extra-territorial CSIS warrant can apply to the activities of Canadians who are terrorist suspects whereas CSE will be limited by its mandate to collect foreign intelligence. CSE intelligence gathered under a Ministerial authorization is less likely to be admitted as evidence than CSIS intelligence gathered under a judicial warrant.

Even if the use of an intelligence intercept or a Criminal Code wiretap was found by the courts to result in an unjustified violation of rights against unreasonable search and seizure, the evidence obtained could in some cases still be admitted into a criminal trial under s.24(2) of the Charter. The *Parmar* prosecution might have continued had the state been able to rely on section 24(2). The state could have argued that it relied in good faith on the warrant even if the warrant could not be sustained and was invalid after the information in the affidavit that identified the informant was edited out. Section 24(2) will not, however, work in all cases and might not have worked in *Parmar* if the court had concluded that there was a serious violation of the Charter.

4. Greater Use of Source and Witness Protection Programs

A final front-end strategy to make intelligence more usable in criminal prosecutions is the use of enhanced witness protection programs by both security intelligence agencies and police forces. Such programs are designed to make it possible for confidential informants when necessary to have their identity disclosed and to testify in criminal prosecutions. They should also when necessary provide protection to informants who may not testify but whose identity might be revealed by

disclosure requirements. The *Parmar* prosecution collapsed because of the unwillingness of a key informant to have his identity disclosed. Many of the disclosure problems in the *Khela* prosecution stemmed from the apparent agreement of the police that the key informant would not have to testify. Informants have many good reasons not to testify and there is no magic solution. Nevertheless, all reasonable efforts should be made to make it possible and attractive for them to testify.

Security intelligence agencies should be able to draw on the resources of witness protection programs. International relocation may be especially important in international terrorism prosecutions. Increased efforts should be made to ensure that the difficulties faced by witnesses are better understood by all. The importance of adequate and effective source and witness protection in managing the relation between evidence and intelligence cannot be easily overstated.[675]

E) Back-End Strategies To Reconcile The Demands of Disclosure and Secrecy

Although front-end strategies to make intelligence more usable in criminal prosecutions need to be developed, there is also a need for back-end strategies that can prevent the disclosure of information that if disclosed will result in serious harm. The disclosure of secret intelligence that is not necessary to ensure a fair trial should not occur given the compelling need to protect informants, security intelligence investigations and operations and the vital free flow of secret information from our allies. Whereas the burden of devising and implementing front-end strategies to make intelligence more useable in terrorism prosecutions fall largely on intelligence agencies and the police, the burden of back-end strategies generally fall on prosecutors, defence counsel, courts and legislatures.

1. Clarifying Disclosure and Production Obligations

One back-end strategy is to clarify the extent of disclosure requirements on the Crown and to provide legislative guidance for requests for

---

675 The most recent annual report on the federal witness protection run by the RCMP indicates that $1.9 million was spent on it and while fifty-three people were in the program, fifteen witnesses refused to enter it, twenty-one voluntarily left the program and seven were involuntarily removed from the program. Witness Protection Program Annual Report 2005-2006 at http://securitepublique.gc.ca/abt/dpr/le/wppa2005-6-en.asp See also Yvon Dandurand "Protecting Witnesses and Collaborators of Justice in Terrorism Cases" in vol 3 of the Research Studies.

production from CSIS when it is determined to be a third party not subject to *Stinchcombe*. A number of the terrorism prosecutions examined in this study were undertaken before the Supreme Court's landmark decision in *Stinchcombe* which requires disclosure of relevant and non-privileged evidence or the Court's recognition in *O'Connor* of a procedure for producing and disclosing material from third parties when required for a criminal trial. Although disclosure standards existed under the common law before *Stinchcombe*, there is a need for as much clarity as possible about the extent of disclosure requirements. Some clarity has been achieved as a result of the amendments governing the opening of the sealed packet under Part VI of the Criminal Code, but more work remains to be done. In its late 1990's study of RCMP/CSIS co-operation, SIRC reported perceptions that any information that CSIS passed to the RCMP would be subject to *Stinchcombe* disclosure requirements. Although *Stinchcombe* imposes broad disclosure obligations, those obligations are not unlimited. The Crown need only disclose information that is relevant to the matters raised in the prosecution. The standard of relevance is higher with respect to *O'Connor* demands for production from third parties. In addition, some balancing of interests is allowed before disclosure of third party records. Information protected by privilege such as the informer privilege, is generally not subject to disclosure. Disclosure can be delayed for legitimate reasons relating to the safety of witnesses and sources and ongoing investigations. Finally, the courts have distinguished between violations of rights to disclosure and more serious violations of the right to full answer and defence.

There is a need for better understanding and codification of disclosure principles. Given the breadth of terrorism offences and the value of having universal rules that apply to all crimes, it may be advisable to codify disclosure principles for all prosecutions. *Stinchcombe* was decided more than fifteen years ago and even at that time, the Court seemed to expect some subsequent codification of the details of disclosure. Greater certainty about the ambit of disclosure requirements and the legitimate reasons for not disclosing information would assist in terrorism prosecutions. The comparative experience of the United Kingdom suggests that there may be considerable advantage in codifying disclosure obligations. The courts in that country proclaimed broad common law standards of disclosure in part out of a recognition that a failure to make full disclosure had resulted in miscarriages of justice in a number of terrorism cases. Parliament, however, subsequently clarified disclosure obligations and the Crown now need not disclose material in any case, including secret intelligence

in terrorism cases, unless it can reasonably be capable of undermining the case for the prosecution against the accused or of assisting the case for the accused.[676] In short, it is not necessary in the United Kingdom to disclose unused but incriminating intelligence.

It will be more difficult to codify and restrict disclosure standards in Canada than in the United Kingdom because the courts have held that the accused has a constitutional right under s.7 of the Charter to disclosure of relevant and non-privileged information. The courts will accept the need to protect legitimate secrets as an objective that is important enough to justify restricting Charter rights, but the critical issue will be whether restrictions on disclosure are the most proportionate means of advancing this important objective. Courts may well look to the process under ss.37 and 38 of the CEA as a less drastic and more tailored means to secure non-disclosure of secrets by judicial order after a judge has examined the secret material in light of the facts of the particular case.

It is also possible for Parliament to legislate in relation to the procedure and standards to be applied when the accused seeks production and disclosure of records held by third parties. Although CSIS was held to be subject to *Stinchcombe* in the unique circumstances of the Air India investigation, it may be held to be a third party in other cases. Legislation to deem CSIS to be a third party not subject to *Stinchcombe* is also a possibility, but one that could be challenged under s.7 of the Charter on the facts of individual investigations. In cases where CSIS is a third party not subject to *Stinchcombe*, the Court in *Mills* made clear that Parliament can alter the common law procedure in *O'Connor* which requires the accused to show that material is likely relevant and that the interests in disclosure are greater than the interests in non-disclosure. For example, it might be possible to clarify that matters relating only to the internal workings of intelligence agencies are not relevant enough to require disclosure to the defence. It may also be possible to instruct courts to consider certain factors, such as the harmful effect of disclosure on informants, commitments made to foreign states and ongoing investigations before ordering production and disclosure. Nevertheless, any new scheme to govern the production of intelligence would have to comply with the accused's right to full answer and defence.

---

676 *R v Ward* [1993] 1 WLR 61; *Criminal Procedure and Investigations Act 1996* s.3 as amended by *Criminal Justice Act 2003; R. v. H and C* [2004] UKHL 3 at para 17.

The courts have already accepted that not every violation of the accused's right to disclosure will violate the even more fundamental right of full answer and defence. The courts may be prepared to accept some legislative limits on disclosure rights, especially when disclosure would harm state interests in national security. That said, the courts are also attentive to the cumulative adverse effects on the accused's right to full answer and defence when the accused is denied access to relevant information and information that could open up avenues for the defence. It is important that independent judges be the ultimate decision-maker about the disclosure of information because state officials have an incentive to maximize secrecy. As a result of noble-cause corruption or tunnel vision, state officials may fail to disclose information that may be valuable to the accused. A failure to make full disclosure has been an important factor in wrongful convictions, including in terrorism cases.

Legislative restrictions on disclosure or production will be challenged under the Charter. Even if upheld under the Charter, the accused will frequently argue that the state has failed to satisfy disclosure or production obligations codified in new legislation. Such arguments could delay terrorism prosecutions. Courts will not and should not return to earlier practices of ordering non-disclosure of intelligence material without even examining the material to determine its value to the accused.

2. Clarifying and Expanding Evidentiary Privileges that Shield Information from Disclosure

A related strategy to reduce disclosure and production obligations is the codification and expansion of privileges like the police informer privilege or the creation of a new privilege. There may be a case for some codification and perhaps expansion to make clear that CSIS informers also enjoy the benefit of police informer privilege, but there are limits to this strategy. Even the most zealously guarded privileges such as the police informer privilege are subject to innocence at stake exceptions.[677] There is an understandable reluctance to create new class privileges and case-by-case privileges may provide little advance certainty about what is not to be disclosed. There is also a danger that new privileges will encourage the non-disclosure of information that is necessary for full answer and defence. If privileges are dramatically expanded, courts

677 *R. v. Leipert* [1997] 1 S.C.R. 287; *Named Person v. Vancouver Sun* 2007 SCC 43.

will likely make increased use of innocence at stake or full answer and defence exceptions to the expanded privilege. The end result may be that an expanded privilege may be less certain and perhaps even less protective of the state's interest in non-disclosure.

Placing too much reliance on legislating narrower disclosure or production rights or expanding privileges may invite both Charter challenges and litigation over whether information fits into the new categories. Rather than attempting the difficult task of imposing abstract limits in advance of the particular case on what must be disclosed to the accused and risking that such limits may be declared unconstitutional or spawn more litigation, a more practical approach may be to improve the efficiency of the process that is used to determine what must be disclosed and what can be kept secret within the context of a particular criminal trial. That said, presumptive privileges could have the benefit of providing some certainty to the agencies, in particular CSIS, that information could be shared with the police without necessarily being disclosed. Any new privilege would have to be defined with as much precision as possible and it would be subject to litigation to determine its precise ambit. It should also be subject to an innocence at stake exception.

3. Use of Special Advocates to Represent the Interests of the Accused in Challenging Warrants while Maintaining the Confidentiality of Information Used to Obtain the Warrant

Electronic surveillance can provide some of the most important evidence in terrorism prosecutions, especially in cases where it may be difficult and dangerous to use human sources. Both the *CSIS Act* and the *Criminal Code* provide means to obtain wiretap warrants. Both provisions have been sustained under the Charter, but courts have stressed that the general rule is that there should be full disclosure of the affidavits used to obtain the wiretap warrant. The affidavit can be edited to protect a broad range of public interests in non-disclosure including the protection of informants and ongoing investigations. This protection of information from disclosure, however, comes with a price. Any material that is edited out of the affidavit and not disclosed to the accused or perhaps summarized for the accused cannot be used to support the legality and constitutionality of the wiretap. Material that has been edited out and not known to the accused cannot be effectively challenged by the accused. In some cases, the editing may mean that the warrant is not sustainable and that the wiretap evidence can only be admitted if a judge determines that its

admission would not bring the administration of justice into disrepute under s.24(2) of the Charter.

The use of security-cleared special advocates in proceedings to challenge wiretap warrants may make it possible to provide adequate protection for the accused's right to challenge the warrant as part of the accused's right to full answer and defence and right against unreasonable searches while not disclosing to the accused information that would compromise ongoing investigations, confidential informants or secret intelligence. Special advocates at present play a role under immigration law security certificates, but the role that they could play with respect to challenging warrants could be less problematic. Special advocates would be standing in for the accused only for the limited purpose of challenging the search and arguing that the evidence should be excluded. [678] A special advocate should be in a good position to make an effective adversarial challenge to the warrant. Indeed, the special advocate could be in a better position than the accused to challenge the warrant to the extent that the special advocate sees information that would normally be edited out. Finally, any evidence that the Crown would lead in a terrorism prosecution, including the results of a wiretap should it be found to be admissible, would still have to be disclosed to the accused to ensure a fair trial. Special advocates could act in the accused's interests in challenging the warrant, but they would not act for the accused during the actual trial.

A security-cleared special advocate could be given full access to the unedited affidavit used to obtain a warrant whereas now the accused only sees an edited version of the affidavit. The special advocate could also have access to other material that is relevant to challenging the wiretap warrant, including *Stinchcombe* material disclosed to the accused. The special advocate could in appropriate cases conduct cross-examinations on the affidavit. The special advocate's access to the full affidavit would respond to the concerns of the Supreme Court that the editing of the affidavit while necessary to protect important law enforcement interests, should be kept to a minimum.[679] The special advocate could be briefed by the accused's lawyer about the case before the challenge to the warrant started. The special advocate could also under existing practice seek the

678 The Supreme Court has stressed the differences between proceedings where the basis for granting a warrant are challenged and a trial on the merits where the accused has full rights of cross-examination and the Crown must prove guilt beyond a reasonable doubt. *R. v. Pires; R. v. Lising* [2005] 3 S.C.R. 343 at paras 29-30.

679 *R. v. Durette* [1994] 1 S.C.R. 469

permission of the presiding judge to ask relevant questions of the accused or his counsel in order to challenge the warrant if this was necessary after the special advocate had seen the unedited affidavit. Such a process would have to be done with care particularly if the special advocate's questions could reveal the identity of an informant or an ongoing investigation. The use of a special advocate could allow the trial judge (who would also have to be authorized to see and hear the secret material) to hear full and informed adversarial challenges to the warrant without disclosing confidential information used to obtain the warrant to the accused or to the public. Information from the warrant that was admitted into evidence in the criminal trial would continue to be disclosed and challenged by the accused and not the special advocate.

4. Confidential Disclosure and Inspection of Relevant Intelligence

At present, lawyers for the accused are placed in the difficult position of making very broad claims for disclosure of intelligence that they have not seen. As will be seen in the next section, the accused's overbroad claims for disclosure are sometimes met with similarly overbroad claims of secrecy. The relation between intelligence and evidence may become more solid if both sides can be encouraged to make more informed and disciplined claims.

In the *Malik and Bagri* prosecution, defence counsel were allowed to inspect CSIS material on an undertaking that they would not disclose the information to their clients unless there was agreement with the prosecutors or a court order for disclosure. Agreement about disclosure was reached in that case and it was not necessary to litigate these issues in the Federal Court under s.38 of the CEA. In future cases, it may be advisable to allow defence counsel to be able to inspect secret material subject to an undertaking that they will not share that information with their client until disclosure has been approved by the Attorney General of Canada or the court. In such cases, there will be a need to ensure the confidentiality of the material that is disclosed and this may require the defence counsel to be provided with access to secure locations and secure equipment.

There may also be a case for requiring defence counsel to obtain a security clearance before obtaining access to secret material. Such a process could delay prosecutions and adversely impact choice of counsel. These problems should not be insurmountable if there is an experienced cadre

of defence lawyers with security clearances and with adequate facilities and funding to conduct a defence. Security clearances for defence lawyers are used in both Australia and the United States. Some of Canada's new special advocates also act as defence counsel.

In cases where a defence lawyer is not willing or able to obtain a security clearance, a security-cleared special advocate could be appointed to see the secret information and challenge the Attorney General's *ex parte* submissions for non-disclosure.[680] The appointment of a special advocate would also add further delay to s.38 proceedings, albeit delay related to becoming familiar with the case and not with respect to obtaining a security clearance. The special advocate may never be as familiar with the possible uses of the undisclosed secret information to the accused as the accused's own lawyer. A special advocate could, however, effectively challenge overbroad claims of national security confidentiality and in that way produce material that could be disclosed to the accused. A special advocate would not be used, as is the case under immigration law, to challenge evidence that is not seen by the accused.[681] As the Supreme Court recognized in *Charkaoui*, s.38 of the CEA does not authorize the use of secret evidence not seen by the accused. Any extension of the use of secret evidence to criminal proceedings would violate the accused's right to a fair trial under ss.7 and 11(d) of the Charter. It would be difficult if not impossible to justify under s.1 given the more proportionate and more fair alternatives of obtaining selective non-disclosure orders on the basis of harms to national security or of prosecuting the accused for another terrorism or criminal offence that would not require the use of secret evidence.

Although special advocates may play a valuable role in s.38 proceedings before the Federal Court in challenging the government's case for secrecy and non-disclosure, it is not clear what, if any, role they would play when a criminal trial judge has to decide under s.38.14 whether

---

680 *Canada . v. Khawaja* 2007 FC 463. See also *Khadr v. Canada* 2008 FC 46 and *Canada v. Khawaja* 2008 FC 560 appointing a security cleared lawyer in s.38 proceedings.

681 The joint committee of the British House of Lords and House of Commons On Human Rights has been critical of the use of special advocates in other contexts, but has concluded that they are appropriate in the similar context of applications for public interest immunity. It has stated: "Public interest immunity decisions are not about whether the prosecution has to disclose the case on which it relies to the defence; rather, such decisions concern whether the prosecution is obliged to disclose material on which it does not rely, which might assist the defence. When deciding a public interest immunity claim, recourse can be had to court appointed special advocates." Joint Committee on Human Rights *Counter-Terrorism Policy and Human Rights: Prosecution and Pre-Charge Detention* July 24, 2006 at para 105.

a remedy is required to protect the accused's fair trial rights in light of the Federal Court's non-disclosure order. The security-cleared special advocate will have seen the secret information that was the subject of the non-disclosure order, but under the present law will not be able to inform the criminal trial judge about this information. The accused will not be subject to such restrictions, but will not have seen the information that was the subject of the non-disclosure order. The process would be simplified if the trial judge was allowed to see the secret information that was the subject of the non-disclosure order.

5. A Disciplined Harm-Based Approach to Secrecy Claims

There is a danger that overbroad demands for disclosure by the accused in terrorism prosecutions may be matched by overbroad demands for secrecy by the Attorney General of Canada. There have been a number of recent disputes over whether the Attorney General of Canada has engaged in overclaiming of national security confidentiality. The disputes between the Arar Commission and the Attorney General of Canada were resolved during the inquiry and by a decision of the Federal Court that authorized the release of the greater part of the disputed information.[682] Over use of national security confidentiality claims can produce public cynicism and suspicion about even legitimate claims of secrecy. When there are legitimate secrets that must be kept to protect vulnerable informants, ongoing investigations and promises to allies, there is a danger that the wolf of national security confidentiality may have been cried too often.

One means of addressing concerns about the legitimacy of national security confidentiality claims would be to narrow the ambit of s.38 which requires justice system participants to invoke its processes over a wide range of material that the government is taking measures to safeguard even if there is not a potential for actual injury to a public interest. Another means would be to specify the precise harms of disclosure to the public interest. Section 38.06 at present requires that the disclosure of the material would be injurious to national security, or national defence or

---

682 *Canada v. Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar* 2007 FC 766. See also *Canada v. Khawaja* 2007 FC 490 and *Canada v. Khawja* 2008 FC 560 for expression of concern that the government has made secrecy claims where injury to national security from disclosure has not been established.

international relations. The courts have attempted to define these terms,[683] but they remain extremely broad and vague. More precise definition of the harms of disclosure, or even specific examples of harms to national security or international relations, might help prevent overclaiming. It could also educate actors about the legitimate needs for secrecy with respect to matters such as the protection of vulnerable sources, ongoing investigations and promises made to allies that intelligence would not be disclosed or used in legal proceedings. A harm-based approach could respond to the concerns articulated by the Arar commission and some judges that the government has invoked s.38 in situations where the injury that would be caused by disclosure has not been established.

Section 38 could also be amended to recognize the evolving distinction between intelligence and evidence. The third party rule should not apply if the information was already in the public domain or known to Canadian officials. Even when the third party rule applies, the government could be required to make reasonable efforts to obtain consent from the originating agency to the disclosure of the caveated material. Courts have also recognized that claims that evidence should not be disclosed because of the "mosaic effect" should be approached with caution. [684] Concerns about the mosaic effect have their origins in the Cold War and may not be as applicable in prosecutions of loosely organized non-state actors such as terrorists. Finally, the harms of non-disclosure could be specified especially in relation to the right to full answer and defence. Attention should be paid to the cumulative effects of non-disclosure on the ability of the accused to undermine the Crown' case and advance defences, as well as on the fairness of the process.

A more restrained and harm-based approach to secrecy claims under s.38 of the CEA, perhaps accompanied by a willingness to allow defence counsel to inspect some secret material on condition of not disclosing the material to their clients without further agreement and perhaps after obtaining a security clearance, could decrease the need to litigate secrecy and disclosure issues under s.38 of the CEA. That said, the Attorney General of Canada will have to insist that some secret material not be disclosed

683 National security has been defined the "means at minimum the preservation in Canada of the Canadian way of life, including the safeguarding of the security of persons, institutions and freedoms" *Canada v. Commission of Inquiry* 2007 FC 766 at para 68. National defence includes "all measures taken by a nation to protect itself against its enemies" and "a nation's military establishment". International relations "refers to information that if disclosed would be injurious to Canada's relations with foreign nations." Ibid at paras 61-62.

684 ibid; *Canada v. Khawaja* 2007 FC 490

and the competing interests in disclosure and non-disclosure will have to be determined under s.38. It is important that the process for reconciling the interests in disclosure and non-disclosure be both fair and efficient.

6. An Efficient and Fair One Court Process for Determining National Security Confidentiality Claims

In my view the most important back-end strategy in managing the relationship between intelligence and evidence is to make the process for seeking non or modified disclosure orders in individual case more efficient and more fair for all parties. Such a reform will respond to the limits of front-end strategies in making it easier to use intelligence as evidence as well as responding to the limits of attempts to reduce disclosure requirements through legislation or the creation of new privileges. The s.38 process should evolve to allow trial judges to decide on the facts of the particular case whether and when disclosure of secret material is necessary for a fair trial. Such an approach follows the best practices of other democracies with more experience with terrorism prosecutions than Canada.

Although public interest immunities can be asserted before superior court trial judges under s.37 of the CEA, national security, national defence and international relations claims can only be asserted before the Federal Court under s.38 of the CEA. Criminal trial judges must respect the orders made by the Federal Court with respect to disclosure, but they also retain the right to order whatever remedy is required, including a stay of proceedings, to protect the accused's right to a fair trial. The *Kevork*, *Ribic* and *Khawaja* case studies underline the difficulties of Canada's two court structure. Although the trial judge in *Kevork* ultimately held that a fair trial was possible after the Federal Court refused to order the disclosure of CSIS material, he expressed much uneasiness about the bifurcated process. It is inherently difficult to ask a trial judge to conclude that disclosure of information that he or she has not seen is not necessary to ensure the fairness of the trial. At a minimum some way must be found to ensure that the trial judge and perhaps a security cleared lawyer can examine relevant secret information that has not been disclosed to the accused.

The *Ribic* prosecution demonstrates that s.38 issues can arise in the middle of a trial. In that case, a mistrial was declared when the issues were litigated in Federal Court and an appeal heard by the Federal Court of Appeal. A new trial was held, but the entire process took six

years to complete. Section 38 was amended in 2001 to require pre-trial notification of an intent to disclose or call classified information. Despite best efforts by all concerned, however, s.38 issues can emerge later in a criminal trial. For example, the Crown has a reviewable discretion to delay disclosure if required to protect witnesses. The accused may also wish to call evidence that might implicate s.38 of the CEA. A trial judge may have difficulty denying the accused the ability to call evidence that is necessary for full answer and defence. Although the Crown could be penalized for late disclosure, a refusal to allow the Crown to make a s.38 claim with respect to late-breaking disclosure could force it to abandon the prosecution in order to keep the information secret. The litigation of national security confidentiality claims in the Federal Court either before or during a criminal trial can threaten the viability of a terrorism prosecution. The accused has a right to a trial in a reasonable time and the public, including the jury, has an interest in having terrorism trials resolved in a timely manner. The delays in the *Khawaja* prosecution are a matter of concern especially when compared to completion of the trial of his alleged co-conspirators in Britain.

Even if delay problems can somehow be avoided through an expedited s.38 process, the two court approach places both the Federal Court and trial judges in difficult positions. The Federal court judge must attempt to determine the importance of non- disclosed information to the accused when the accused's lawyer has not seen the information and at a pre-trial stage when the issues that will emerge at trial may not be clear. The ability of the defence to make *ex parte* submissions to the Federal Court judge cannot compensate for the fact that the defence has not seen the undisclosed evidence and the trial evidence has not yet taken shape. Even the possibility that a security cleared special advocate may be appointed to challenge the government's case for non-disclosure cannot guarantee the disclosure of all information that should be disclosed. Even if the Federal Court judge had the advantage of full adversarial arguments on non-disclosure motions, the judge would still have the burden of making final decisions about non-disclosure and partial disclosure without knowing how the criminal trial might evolve. Judges who make similar non-disclosure decisions in Australia, the United Kingdom and the United States all take great comfort in the fact that they can revisit their non-disclosure decisions in light of emerging evidence and issues at trial.

The criminal trial judge is in an equally difficult position under the unique two court structure of s.38 of the CEA. The trial judge must decide that a

fair trial is possible without the disclosure of information that the accused, the accused's lawyers and likely the trial judge have not seen. Conversely, the trial judge must fashion a remedy, including perhaps a stay of proceedings, for non-disclosure of the secret information. Although the trial judge might be guided by a schedule that lists the information that was subject to the non-disclosure order, that schedule itself cannot contain identifying information that would cause injury to national security or national defence or international relations.[685] Although the trial judge can issue a report to the Federal Court judge under s.38.05 and the Federal Court can apparently remain seized of the s.38 matter during the trial, [686] the two court structure remains cumbersome and unprecedented outside Canada.

One possible argument in favour of the present two court system is that it provides a form of checks and balance between the two courts and ensures that the trial judge is not tainted by seeing the secret information that the Federal Court has ordered not be disclosed. No concerns have, however, been raised in other countries that judges will be influenced in their decisions by the information that they have seen, but ordered not to be disclosed. In many cases, the material will simply be intelligence that the Crown has found not to be necessary to be used as evidence. Judges are routinely trusted to disregard prejudicial but inadmissible information about the accused including coerced or unconstitutionally obtained confessions. In any event, the accused will also have the right to a trial by jury.

Canada's unique two court approach runs the risk of decisions in both the Federal Court and the trial court that either prematurely decide that disclosure is not necessary or alternatively that prematurely penalize the prosecution for failing to make disclosure that is not actually required in order to treat the accused fairly. In short, the bificurated court structure is a recipe for delay and disaster in terrorism prosecutions.

No other democracy of which I am aware uses a two court structure to resolve claims of national security confidentiality. Australia, the United Kingdom and the United States all allow the trial judge to decide whether sensitive information can be withheld from disclosure without compromising the accused's rights. This approach is attractive because

685 *Canada. v. Khawaja* 2007 FCA 342 at para 12.
686 *Canada v. Khawaja* 2008 FC 560.

it allows trial judges to make non-disclosure orders knowing that they can revise such orders if fairness to the accused demands it as the trial progresses.

A One Court Approach: Superior Trial Court or Federal Court?

Reforms of the two court Canadian approach could proceed in two directions. It is perhaps possible to give the Federal Court jurisdiction over all terrorism prosecutions. This approach, however, would require that the Federal Court be given jurisdiction to sit with a jury or it would attract challenge under s.11(f) of the Charter. The expansion of Federal Court jurisdiction or an attempt to create a new court to hear terrorism cases could also attract challenge under s.96 of the Constitution Act, 1867 as infringing the inherent core criminal jurisdiction of the provincial superior courts. The expansion of Federal Court jurisdiction to include criminal terrorism trials or the creation of a new terrorism court could be supported by an argument that terrorism, like youth justice, is a novel matter that did not exist in 1867. As such, it could be transferred away from the superior trial courts.[687] Nevertheless, there are stronger arguments that terrorism has been around for a long time and that terrorism prosecutions in essence involve attempts to punish murder including conspiracy and attempted murder. From 1867 to the present, only superior trial courts in the provinces have tried murder charges before juries.[688] Murder, like contempt of court and perhaps treason, sedition, and piracy, are matters within the core jurisdiction of the superior trial courts in the provinces. As such, they cannot be changed by Parliament or the provinces without a constitutional amendment. Removing jurisdiction from the provincial superior courts to try the most serious crimes, terrorist acts of murder or preparation or facilitation of such acts, could be held to violate s.96 of the Constitution Act, 1867.[689] The Federal Court or a new terrorism court would still be conducting terrorist trials for traditional purposes of determining guilt and punishment as opposed to distinct purposes such as developing a system of youth justice. Even if s. 96 did not prevent a transfer of core superior court jurisdiction to another federal court, the

687 *Reference re Young Offenders* [1991] 1 S.C.R. 252.

688 See *Criminal Code* s.469.

689 *MacMillan Bloedel Ltd. v. Simpson* [1995] 4 S.C.R. 725 at para 15 ("The superior courts have a core or inherent jurisdiction which is integral to their operations. The jurisdiction which forms this core cannot be removed from the superior courts by either level of government, without amending the Constitution).
(emphasis added) The dissent rejected the idea of core jurisdiction in that case, but also found that jurisdiction being removed from the provincial superior court to punish young people for contempt of court was ancillary to special powers exercised by youth courts.

power to constitute courts of criminal jurisdiction to try terrorism crimes is arguably a matter of provincial jurisdiction.[690]

Even if constitutionally permissible, such an approach would also require the Federal Court to develop and maintain expertise in criminal law, criminal procedure and criminal evidence matters. This could be difficult if terrorism prosecutions remain infrequent. A former general counsel to the Central Intelligence Agency, Fred Manget, has rejected calls for the Foreign Intelligence Surveillance Court (which issues foreign intelligence wiretaps) to conduct criminal terrorism prosecutions. He has argued that although the special court "operates with admirable secrecy, it was not meant to conduct trials. Instead, it was designed to establish the existence of probable cause, based only upon the government's ex parte appearance. Mixing the probable cause determination with an adversarial trial could raise due process or impugn the impartiality of subsequent trials."[691] In other words, it is better to build national security expertise into the existing criminal trial courts than to attempt to give a court with national security expertise but no criminal trial experience the difficult task of hearing terrorism trials.

Having terrorism prosecutions heard in the Federal Court or the creation of a new court would also raise concerns about special terrorism courts, concerns that have surrounded the Diplock courts in Northern Ireland and special courts in Ireland. One of the values of terrorism prosecutions is that they allow terrorist acts of violence to be denounced as crimes and terrorists to be punished and stigmatized as criminals. At this level, at least, terrorists should not be elevated to the status of a political challenge to the state that requires special solutions such as special courts.

A preferable approach would be to give designated judges of the superior trial court who have extensive experience with complex criminal trials the ability to determine national security confidentiality claims under

---

690 Peter Hogg has suggested that s.96 should not prevent the transfer of core superior court jurisdiction to another federal court. Peter Hogg *Constitutional Law of Canada* 4th ed at 7.2(e) But *MacMillan Bloedel Ltd. v. Simpson* [1995] 4 S.C.R. 725 at para 15 indicates that the core jurisdiction of the superior courts "cannot be removed from the superior courts by either level of government, without amending the Constitution." In any event, Professor Hogg also indicates that the federal government does not have jurisdiction to constitute or establish courts of criminal jurisdiction, a matter expressly excluded from the federal power over criminal law and procedure under s.91(27) and included in the provincial power over the administration of justice under s.92(14). See ibid at 19.3. The only federal power that would support the creation of a new court to try terrorism cases would seem to be the somewhat uncertain residual power to make laws for peace, order and good government.

691 Fred Manget "Intelligence and the Criminal Law System" (2006) 17 Stanford Law and Public Policy Review 415 at 428.

s.38 of the CEA during a terrorism trial. This could be done by amending the definition of a judge under s.38 to include a judge of the provincial superior court when a national security confidentiality matter arises before or during a criminal trial. Because of the need for secure facilities and training with respect to national security confidentiality, not all provincial superior court judges would have to be designated as judges under s.38 of the CEA. The Chief Justice of each provincial superior court could designate a few judges who would be able to make decisions under s.38 of the CEA for the purposes of criminal trials. This could also have the effect of allowing such a trial judge to be assigned to a terrorist case at the earliest possibility in order to help case manage complex terrorism prosecutions.

Superior court trial judges can already decide public interest immunity claims under s.37 and they should be able to learn enough about national security matters to make s.38 decisions. The Attorney General of Canada would still have the opportunity to make ex parte arguments to these judges about the dangers of disclosing information. These judges could also be assisted by adversarial argument on s.38 issues provided by the accused and by security-cleared special advocates who had examined the secret material. Finally, the Attorney General of Canada would still have the power under s.38.13 of the CEA to block a court order of disclosure of material that relates to national security or national defence or was received from a foreign entity.

It could be argued that the Federal Court should retain responsibility in all s.38 matters because of its expertise and the need to reassure allies that secret information will be treated with appropriate care. If this argument was accepted, it would still be possible to appoint select provincial superior courts judges as deputy judges of the Federal Court with the consent of their Chief Justice, the Chief Justice of the Federal Court and the Governor in Council.[692] Such judges would have to acquire expertise with respect to matters affecting national security confidentiality.[693] In addition, it might be easier for provincial superior court trial judges who were designated as deputy judges of the Federal Court to use the secure facilities of the Federal Court.

---

692 *Federal Court Act* s.10.1.

693 The designated judges could perhaps also consider CSIS warrant requests in order to maintain their experience should terrorism trials involving s.38 issues prove to be rare.

Allowing provincial superior court trial judges designated by their Chief Justice to decide national security confidentiality or public interest immunity questions would be consistent with the approaches taken in Australia, the United Kingdom and the United States. Such an approach could develop specialized expertise among a small number of trial judges with respect to all aspects of the management of terrorism trials including s.38 issues.[694] Measures would have to be taken to ensure that superior court trial judges designated to decide s.38 issues that arise in a criminal trial would have the appropriate facilities and training for the storage of classified information and that they would have the opportunity to develop expertise on complex matters of national security confidentiality. If necessary, terrorism trials could under s.83.25 of the Criminal Code be prosecuted by the Attorney General of Canada in Ottawa, even if the offence is alleged to have been committed outside of Ontario.

This single court approach would allow trial judges to manage all disclosure aspects of complex terrorism prosecutions without artificial separations between s.38 matters that have to be decided in the Federal Court and other disclosure matters including those under s.37 that have to be decided by the trial judge. It would also stop the duplication of proceedings that may be caused by having preliminary disputes and appeals decided under s.38 only to have the same or similar issues potentially resurface before the trial judge under s.37 or s.38.14 of the CEA. A one court approach could help establish a solid institutional foundation for managing the difficult and dynamic relationship between secret intelligence and information that must be disclosed to the accused.

7. Abolishing Pre-Trial Appeals

A final reform to make the national security confidentiality process more efficient would be to repeal s.38.09 of the CEA which allows for decisions about national security confidentiality to be appealed to the Federal Court of Appeal with the possibility of a further appeal to the Supreme Court of Canada under s.38.1. The criminal trial process has traditionally avoided appeals of issues before or during a criminal trial because of concerns about fragmenting and delaying criminal trials.

An accused would retain the ability to appeal a non or partial disclosure

694 It could be argued that existing Federal Court judges with expertise in national security matters should also be allowed to conduct criminal trials. This, however, would require cross-appointing such judges to multiple provincial superior courts.

order as part of an appeal from a conviction to the provincial Court of Appeal as contemplated under the Criminal Code. It could be argued that the provincial Courts of Appeal do not have expertise in matters of national security confidentiality. Provincial Courts of Appeal already hear public interest immunity appeals under s.37 of the CEA. They could take guidance from the s.38 jurisprudence that has been developed and would continue to be developed in the Federal Court in non-criminal matters. Finally, the Supreme Court of Canada maintains the ultimate ability to interpret s.38 for all courts. If pre-trial appeals were abolished under s.38, most appeals would involve many matters of criminal law, procedure and evidence that are within the expertise of the provincial Courts of Appeal in addition to the s.38 issue.

The Attorney General of Canada would lose the right to appeal an order authorizing disclosure, a right that it exercised with partial success in *Khawaja*.[695] It could be argued that this might prematurely sacrifice prosecutions by not allowing the Attorney General an opportunity to establish that a judge had committed legal error and ordered too much information disclosed to the accused. Nevertheless, the Attorney General of Canada would retain the right to issue a certificate prohibiting disclosure under s.38.13 of the CEA or of taking over a terrorism prosecution and entering a stay of proceedings should it conclude that the public interest would be seriously harmed by disclosure. The abolition of pre-trial appeals may require closer co-ordination between the Attorney General of Canada and those who handle terrorism prosecutions either in the provinces or through the new federal Director of Public Prosecutions. In any event, there is a need to co-ordinate these processes and the Attorney General of Canada retains the ability to prosecute terrorism offences.[696]

If pre-trial appeals from a s.38 determination are to be retained, however, thought should be given to providing time-limits not only for the filing of appeals, but also for the hearing of arguments and the rendering of decisions.

F) Conclusion

There is an urgent need to reform the process through which national security confidentiality claims are decided. Most of Canada's past terrorism

695 2007 FCA 342. Note however that the error in that case might have been corrected by asking the judge to reconsider his original decision. ibid at paras 18, 52.

696 *Security Offences Act* R.S. 1985 c.S-7, s.2; *Criminal Code* s.83.25.

prosecutions have involved material supplied by Canadian and foreign security intelligence agencies and this trend will likely increase given the nature of international terrorism. Although some front-end reforms may make intelligence agencies more willing to disclose intelligence or even to use intelligence as evidence, some secrecy claims will be necessary to protect vulnerable informants, sources and methods and to respect restrictions on the subsequent disclosure of information.

Although there may be some benefits in codifying disclosure and production requirements, and in attempting to define material that clearly does not have to be disclosed or produced, there is a danger that restrictive disclosure and production requirements will generate Charter challenges and increased litigation over the adequacy of disclosure. It may be wiser to improve the efficiency of the process through which the government can seek orders to prohibit disclosure in specific instances. The 2006 MOU between the RCMP and CSIS contemplates the use of s.38 of the CEA to protect CSIS material. Unfortunately, the use of s.38 can threaten the viability of terrorism prosecutions through delay, pre-trial appeals and through non-disclosure orders by the Federal Court that may require a trial court to stay proceedings.

The parties to the Malik and Bagri prosecution took extraordinary and creative steps to avoid litigating issues under s.38. Such litigation in the Federal Court would have delayed and fractured a criminal trial which was already one of the longest and most expensive in Canadian history. If s.38 had been used in the Malik and Bagri prosecution, it is possible that the prosecution would have collapsed or that a stay of proceedings would have been entered under s.38.14. Proceedings also could have been stayed because of CSIS's failure to retain information that was of potential disclosure and evidential value to the accused. Although Air India was a unique case that hopefully will never be repeated, accused will continue to seek disclosure or production of the work of Canada's security intelligence agencies and information collected by our intelligence agencies may in some cases constitute important evidence in terrorism prosecutions. Front-end reforms designed to make intelligence more usable in terrorism prosecutions and back-end reforms to determine in an efficient and fair manner whether intelligence must be disclosed to the accused are required to respond to the unique and difficult challenges of terrorism prosecutions.

The trial judge should be empowered to make decisions about whether secret information needs to be disclosed to the accused. Such an approach should allow the trial judge to make disclosure and national security confidentiality decisions without the inefficiencies and potential unfairness revealed by separate Federal Court proceedings in the *Kevork, Ribic* and *Khawaja* prosecutions. The judge could decide in cases where the intelligence would not assist the accused that disclosure of the secret information was not necessary while retaining the ability to re-visit that decision if necessary to protect the accused's right to make full answer and defence as the trial evolves. Combined with front-end reforms that prepare intelligence to the extent possible for disclosure and use as evidence, a one court approach would move Canada towards the approaches used in other democracies with more experience in terrorism prosecutions. It would provide a better foundation for management of the difficult and dynamic relationship between secret intelligence about terrorist threats and evidence and information that must be disclosed in terrorist trials.

Without significant reforms, there is a danger that terrorism prosecutions in Canada may collapse and become impossible under the weight of our unique two court approach to reconciling the need for secrecy and the need for disclosure and our old habits of ignoring the evidentiary implications of the gathering of intelligence. An inability to try terrorism prosecutions on their merits will fail both the accused and the victims of terrorism.

Kent Roach is a Professor of Law with cross appointments in criminology and political science. He holds the Prichard and Wilson Chair of Law and Public Policy at the University of Toronto. In 2002, he was elected a Fellow of the Royal Society of Canada by his fellow academics. He was a former clerk for the last Justice Bertha Wilson on the Supreme Court of Canada. He has been the editor in chief of the Criminal Law Quarterly since 1998 and has appeared frequently as counsel for various interveners in the Supreme Court and Courts of Appeal. He is the author of nine books including *Constitutional Remedies in Canada* winner of the 1997 Owen Prize for best Canadian law book and (with R.J. Sharpe) *Brian Dickson: A Judge's Journey* winner of the 2004 Dafoe Prize for book that contributes most to the understanding of Canada. Two other of his books have been shortlisted for the Donner Prize for best public policy work.

In recent years, Professor Roach has focused much of his work on anti-terrorism law and policy. He is the co-editor of *Global Anti-Terrorism Law and Policy* (Cambridge: Cambridge University Press, 2005) and *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001). He is also the author of *September 11: Consequences for Canada* (Montreal: McGill-Queens Press, 2003) and numerous other articles on anti-terrorism law including the 2002 McGill Law Journal Lecture and the 2005 Viscount Bennett Lecture. These lectures were subsequently published in the McGill Law Journal and the Cardozo Law Review respectively. He has appeared before committees of the Canadian Parliament, Indonesia and the United States Congress on matters related to anti-terrorism law and policy. He was also part of a legal expert group for the United Nation's Office on Drug and Crime that examined penal provisions to implement the Convention for the Suppression of Nuclear Terrorism.

Professor Roach's articles on anti-terrorism laws have been published in Australia, Canada, Egypt, Hong Kong, the Netherlands, Italy, Singapore, South Africa, the United Kingdom and the United States and have also been translated into Arabic, Chinese and Russian. He has lectured on anti-terrorism law and policy at the University of Cape Town, the University of New South Wales, the National University of Singapore, Oxford and Yale. He was a member of the five person research advisory panel for the Commission of Inquiry into the actions of Canadian Officials in Relation to Maher Arar and research director for Ontario's Inquiry into Forensic Pediatric Pathology. He served as Director of Research (Legal Studies) for the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.