Threading the Needle: Structural Reform & Canada's Intelligence-to-Evidence Dilemma

CRAIG FORCESE*

FEATURED ARTICLE

ABSTRACT

This article canvasses the "intelligence-to-evidence" dilemma in Canadian anti-terrorism. It reviews the concept of "evidence", "intelligence" and "intelligence-to-evidence" (I2E). It examines Canadian rules around disclosure to the defence: the *Stinchcombe* and *O'Connor* standards and the related issues of *Garofoli* challenges. With a focus on Canadian Security Intelligence Service (CSIS)/police relations, the article discusses the consequences of an unwieldy I2E system, using the device of a hypothetical terrorism investigation. It concludes disclosure risk for CSIS in an anti-terrorism investigation can be managed, in a manner that threads the needle

* Full Professor, Faculty of Law (Common Law Section), University of Ottawa. Email: cforcese@uottawa.ca; Twitter: @cforcese. The author wishes to thank the several people who commented on drafts of this paper. These include Leah West, Peter Sankoff and Philip Wright. This paper also benefited from extended conversations (and past collaboration) on this topic with Kent Roach. My thanks go to the three anonymous peer reviewers whose comments and fresh eyes contributed to this paper's refinement. I am also grateful to the past and present officials in the Government of Canada who discussed with me the issues addressed in this paper – and helped me "ground-truth" the operational reality of CSIS and RCMP investigations. Out of an abundance of caution, I will leave those interlocutors anonymous. Any errors are, of course, my own. But whatever usefulness this paper has stems from the input of these people. Finally, the author would like to thank the Social Sciences and Humanities Research Council for their support of the larger project of which this paper is a product, administered (with my thanks) by the Canadian Network for Research of Terrorism, Security and Society.

between fair trials, legitimate confidentiality concerns and public safety. The paper proposes both administrative and legislative changes accomplishing these objectives.

Keywords: intelligence; evidence; criminal law; national security; terrorism; police; CSIS

I. INTRODUCTION

Canada struggles with terrorism investigations. Not least, the Canadian Security and Intelligence Service (CSIS) and police struggle to coordinate and collaborate. Consider this passage from *Ahmad*, a 2009 terrorism prosecution: "CSIS was aware of the location of the terrorist training camp...This information was not provided to the RCMP, who had to uncover that information by their own means. Sometimes CSIS was aware that the RCMP were following the wrong person, or that they had surveillance on a house when the target of the surveillance was not inside, but [CSIS] did not intervene."[1]

Reasonable observers might assume that CSIS's failure to inform the police was a one-off mistake, or at worst a remnant of the cultural divide that bungled the 1985 Air India bombing investigation. It was not – it exists by design. This design responds to the "intelligence to evidence" (I2E) dilemma, and specifically the risk that sensitive CSIS targets, sources, means and methods might be disclosed to the defence (and public) in a prosecution, should CSIS share its intelligence with the police.

Both inside and outside government, observers now acknowledge the institutional distance created by I2E is a problem, and must be solved. I2E was described by the current CSIS director as one of the most pressing challenges for CSIS,[2] and a former commissioner of the RCMP worried that terrorism investigations are not well coordinated at the structural level to manage public safety risks.[3] But solutions are not easy. Like many issues in

---

1 *R v Ahmad*, 2009 CanLII 84776 (Ont Sup Ct J) at para 43, [2009] OJ No 6153 [*Ahmad*].

2 David Vigneault, "Ep 36: An INTREPID Podsight: CSIS Director David Vigneault" (11 May 2018) at 00h:29m:40s, online (podcast): *A Podcast called INTREPID* <www.intrepidpodcast.com/podcast/2018/5/11/t7a66ktq1pwmscgk9hinevyhu3slcn> [perma.cc/G8F4-EUAJ].

3 Bob Paulson, "EP 41: An INTREPID Podsight: Bob Paulson, former Commissioner of the Royal Canadian Mounted Police" (15 June 2018) at 00h:18m:35s, online (podcast): *A Podcast called INTREPID* <www.intrepidpodcast.com/podcast/2018/6/15/ep-40-an-

national security law, the I2E problem stems from real dilemmas. Solving the issue requires navigating a narrow strait between Odysseus's feared monsters, Scylla and Charybdis. And weaving this path bumps up against stiff currents produced by legal uncertainty, agency culture, cross-agency coordination and simple institutional inertia, all reinforcing each other. In the result, Canada's response to I2E dilemmas have so far been minimalist.

Like others,[4] I do not believe this is a satisfactory strategy. In the past, I have described I2E as the single biggest shortcoming in Canadian anti-terrorism law and policy,[5] and compared it to the tail that wags Canada's domestic anti-terrorism dog. It drives a siloing between police and CSIS, and silos are anathema in a dynamic security environment. The most obvious disaster stemming from siloing would be a terrorist outrage that (whether state actors admit it or not) could have been averted by more seamless intelligence-to-evidence solutions.

Less tragic – but still concerning – outcomes are criminal cases never brought because police and prosecutor right-hands are unable to act on intelligence produced by the CSIS left-hand. A related, sub-optimal outcome would be CSIS unilateralism: confronted with no solution to the I2E conundrum, CSIS responds to a threat with its new threat reduction powers,[6] even where such disruptions simply kick security dangers down the road through episodic disruptions that risk (as is notorious with disruptions) unforeseen knock-on consequences. All these outcomes would degrade security.

---

intrepid-podsight-bob-paulson-former-commissioner-of-the-royal-canadian-mounted-police> [perma.cc/GUK8-LMP6].

4 Intelligence-to-evidence was a central concern of the 2010 Air India Bombing commission of inquiry report. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Final Report*, vol 1 (Ottawa: Public Works and Government Services Canada, 2010), online (pdf): <epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air_india/2010-07-23/www.majorcomm.ca/en/reports/finalreport/volume1/volume1.pdf.> [Air India Inquiry Vol 1]; See also Kent Roach, *The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence,* vol 4 of the Research Studies of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (Ottawa: Supply and Services, 2010).

5 See e.g. Craig Forcese, "Staying Left of Bang: Reforming Canada's Approach to Anti-terrorism Investigations" (2017) 64 Crim LQ 487.

6 Canadian Security Intelligence Service Act, RSC, 1985, c C-23, s 12.1 [CSIS Act] ("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.").

But these consequences would also undermine civil liberties. People are killed or injured in an avertable terror attack, precipitating knee-jerk responses that may do nothing to solve real problems but do fetter liberties. Threat reductions, done under secret warrant and possibly in violation of the law otherwise applicable to CSIS, fuel concerns about overreach, especially when done in the fog of uncertainty, and risk reputational fallout when they go wrong.

In writing this paper, I therefore share the view of others that anti-terrorism must always leave prosecutions on the table. Prosecutions, despite their imperfections, remain the clearest, most transparent and fairest means of responding to a security threat.[7] They signal that the liberal democratic state will respond with the tools of justice, not subterfuge. Following a fair, measured process, convictions denounce and stigmatize in a way nothing else can, a considerable virtue in an area of competing narratives. It is true other tools may be more appropriate than prosecutions in some circumstances. But that is a decision that should be driven by security imperatives, not artificial institutional fetters. Prosecutions should not fall from the toolbox because Canada has feet of clay on intelligence-to-evidence.

So how do we solve I2E? This article argues the first stage in resolving this conundrum is to understand it, and to tease its component pieces apart. Reducing the fog of uncertainty in this area requires a hard look at what the law is, and what it requires. To what degree are intelligence-to-evidence dilemmas the product of unalterable legal impediments? Are there steps that might plausibly be taken without violence to constitutional standards, and if so what path best navigates between the horns of the dilemma?

This article is organized into five sections. The first parts review the concept of "evidence," "intelligence" and "intelligence-to-evidence." Here, I point to the legal context in which I2E arises in Canada. Specifically, I examine Canadian rules around disclosure to the defence: the *Stinchcombe* and O'C*onnor* standards and the related issue of *Garofoli* challenges. With a focus on CSIS/police relations, I then discuss the consequences of an unwieldy I2E system, using a hypothetical terrorism investigation of Bob the Bomb-Builder and his confederates. I conclude the disclosure risk for CSIS in an anti-terrorism investigation can be managed, in a manner that threads the needle between fair trials, legitimate confidentiality concerns and public

---

7 On this point, see Craig Forcese & Kent Roach, *False Security: The Radicalization of Canadian Anti-terrorism* (Toronto: Irwin Law, 2015) at chapter 9.

safety. I propose a three-legged approach to achieving this goal. To invoke another analogy, solving intelligence-to-evidence requires "moneyball": it requires incremental changes in several different areas that cumulatively culminate in regular base hits, rather than infrequent home-runs punctuated with numerous strike-outs.

I end this introduction with a disclaimer: As they consider this article, readers should be conscious of its inevitable shortcomings, especially in its assessment of current government practices. I have spent considerable time talking about this issue with lawyers and security practitioners in government. But I am an academic lawyer who has never worked in that government. Given how little on this subject is part of the public record, I know only what I have been able to extract from use of the access to information law, and from what people have been prepared to tell me. That means that my analysis is likely a close study of the tip of the iceberg.

II. Defining "Evidence"

In my experience, different individuals and agencies debating "intelligence-to-evidence" (or I2E) mean different things by the expression. This uncertainty in diagnosing the problem makes it difficult to imagine solutions. This article begins, therefore, with definitions of "evidence," "intelligence" and "intelligence-to-evidence."

Neither "evidence" nor "intelligence" mean, simply, information. Both evidence and intelligence are purposive concepts; that is, they comprise information marshalled for specific ends. They are, therefore, subsets of information. But the subsets differ, because the purposes that define them also differ.

"Evidence" is the easier, and narrower expression, because it is tied strictly to the legal system and thus confined to the smaller box. Evidence is information, the truth of which determines facts that matter in deciding a legal adjudication. Put another way, evidence is data used by a trier of fact (a judge, adjudicator or jury) to resolve factual controversies.[8] It is information that is relevant because it tends, as a matter of logic or experience, to prove a fact that matters (is material) in the case. "Materiality"

---

[8] In the discussion on materiality and relevance that follows, I draw on the concepts and structure of David M Paciocco & Lee Stuesser, *The Law of Evidence* 7th ed (Toronto: Irwin Law, 2015) at chapter 2.

and "relevance" constitute, therefore, the dual litmus test for deciding when information is "evidence."

A. Materiality and Relevance

A material fact is a fact that a party is trying to prove because it affects the outcome in a case. Alice's eye-witness testimony that she saw Bob build a bomb is evidence of a material fact in a case in which Bob is charged with bomb-making. Alice's eye-witness testimony that Bob enjoys watching *Saturday Night Fever* is information, but it is not evidence because it does not relate to a material fact, at least not without additional context.

Evidence may also have a more "secondary" materiality, because it matters in assessing the quality of the evidence of a directly material fact. For example, if Alice's roommate Sally testifies that Alice is a compulsive liar, Sally's evidence does not have a direct connection to the fact of whether Bob built a bomb. It does, however, create doubt about the reliability and credibility of Alice's testimony, and therefore is connected to the question of whether Alice truly did see Bob build a bomb. It has, therefore, a more indirect materiality.

"Relevance" is closely associated with the concept of materiality. While materiality determines which facts matter (e.g., that Bob built a bomb vs. his misplaced fondness for *Saturday Night Fever*), relevancy is concerned with whether the evidence actually assists in proving the existence (or not) of a fact material to the case. Or put another way, "[r]elevance can be defined as evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."[9] Sometimes, evidence that contributes to proving a fact is also called "probative". Alice's eye-witness testimony "I saw Bob build a bomb" is relevant, because logic and experience suggest that seeing Bob in the act contributes to the probability that Bob did build a bomb (that is, the testimony is probative). Likewise, Sally's direct experience with Alice as a compulsive liar is relevant (and probative), because it diminishes the probability that Alice's evidence proves Bob built a bomb.

In comparison, information concerning Bob's collection of vinyl records is not relevant, as it does not assist (is not probative) in determining the probability of a material fact (i.e., whether Bob built a bomb). This

---

9 *R v P (R)*, (1990) 58 CCC (3d) 334 (Ont H Ct J) at para 9, [1990] OJ No 3418.

irrelevant information is, effectively, "non-evidence" as it does not assist in resolving a factual controversy material to the case.[10] That is, it does not assist in deciding whether a fact that affects the outcome of a case is true or not.

It is not always easy to decide whether evidence is "relevant" to a "material" fact (that is, whether it affects the probability of the existence of a material fact). Relevance is contextual and will vary according to the facts at issue in the case, and what position the parties take on those facts. Evidence that one assumes will be relevant may prove irrelevant. In our hypothetical, any evidence that assists in resolving the fact of whether Bob built a bomb is obviously relevant to a material fact. And so, sales receipts showing that Bob acquired an unusual amount of fertilizer are relevant. But it may not be necessary for the prosecutor to prove the purchase of fertilizer if Bob admits to the purchase. And so, the sales receipts are no longer relevant to a material fact in dispute. The relevance of evidence may also depend on its immediate context. If Bob was playing the terrorist villain on the TV show *24* and Alice only "saw Bob build a bomb" in Episode 14, Alice's evidence suddenly becomes irrelevant.

On the other hand, it is also the case that things that one assumes irrelevant may turn out to be relevant. For instance, Sally's evidence of Alice's relationship with honesty only becomes relevant when Alice's testimony on Bob's conduct is used as evidence for Bob's conduct. In other words, relevance "may become apparent only when other evidence is adduced, and even then, it may depend on a chain of inferences."[11]

For reasons discussed further below, "relevance" is a key consideration in the I2E dilemma. The key take-away here, however, is that "relevant" does not mean <u>every</u> piece of information that might be in the possession of an investigative agency.

B. Other Admissibility Considerations

While the starting point is that all relevant evidence should be available to the trier of fact "in a search for truth,"[12] other (essentially policy) considerations may limit this access, and therefore determine what

---

10 Paciocco & Stuesser, *supra* note 8 at 4. See also *Mitchell v Canada (MNR)*, 2001 SCC 33 at para 30 (to be admissible, "the evidence must be useful in the sense of tending to prove a fact relevant to the issues in the case.").

11 Paciocco & Stuesser, *supra* note 8 at 32.

12 *R v Jarvis,* 2002 SCC 73 at para 68.

information is "evidence." These include legal "privileges" – such as solicitor-client privilege – and the public interest immunities found in section 38 of the *Canada Evidence Act*, discussed further below. These exclusions deny triers of fact access to certain types of information, to preserve other societal interests.

Other rules of evidence restrict the use to which some (even relevant) information may be put, based on suppositions about the reliability of that information. For instance, where it applies, the "hearsay" rule privileges statements made in-court, over those made out-of-court. Because trial fairness is (presumptively) imperiled if a speaker's information cannot be challenged in court, an out-of-court statement made by a person (who cannot be questioned in court) cannot generally be used to prove the truth of what it asserts. The CSIS intelligence office (IO) may assert "the informant told me she saw Bob building a bomb." But unless the informant is produced to testify in court, the IO's statement cannot generally be used to prove that Bob was building a bomb (although the IO could certainly use that tip to justify an investigation into Bob's activities).

To avoid rigid legal formalism, there are, however, exceptions even to this hearsay rule. Most notably, the formal hearsay rule gives way where the statement is reasonably necessary to prove a fact, and it satisfies a qualitative judgment concerning its reliability.[13] This reliability is assessed with "indicia" suggesting the statement is inherently trustworthy, or where its trustworthiness can be tested. Assume, for example, the IO's informant was the night-watchman on his appointed rounds. The latter found Bob building a bomb and then contacted the authorities. He was carefully and thoroughly questioned by the IO in a recorded conservation. The evidence produced in this manner would likely be more trustworthy than if the informant was a trespasser who reported seeing Bob building the bomb only when subsequently questioned by the IO, and now has since disappeared. Of course, a party wishing to rely on hearsay evidence would need to prove the indicia of reliability, increasing the scope of information that now is relevant to the case.

"Opinion evidence" is another sort of information treated with suspicion by the rules of evidence. An opinion is an "inference from observed fact."[14] If Alice says "I saw Bob build a bomb," the obvious

---

13 See discussion in Paciocco & Stuesser, *supra* note 8 at 114.

14 *Ibid* at 195 (The discussion of opinion evidence is drawn from *ibid* Chapter 6, unless otherwise noted).

rejoinder is: "How, Alice, did you know it was a bomb?" Put another way, on what basis did Alice draw her inference that the thing Bob was working on was a bomb? But if Alice says "I saw Bob dismantling and adding components to a pressure cooker," this is a statement of fact (assuming Alice knows what a pressure cooker looks like), and Alice is not offering an opinion of her own. The implications of Bob's conduct are then left to the trier of fact, bolstered by whatever other evidence is offered concerning Bob's objectives (that is, bomb-making). (And in keeping with the discussion of relevance, Bob's employment as a repair person in a kitchen appliance shop now becomes more than information. It is admissible evidence because relevant to a newly material fact.)

The starting point is that facts are admissible, and opinions are not. There are, however, exceptions. Where they are in a better position to do so than the trier of fact, non-expert witnesses ("lay" witnesses) are permitted to offer opinions of a sort that people of ordinary experience can make and where recourse to an opinion is the most effective way of communicating the underlying facts. For example, Alice reporting "the person I saw was Bob" is, strictly speaking, voicing an opinion. But it would ask too much of Alice to expect her to instead testify about the physiographic features of the man's face. (Of course, if Bob contests that it was he that Alice saw, this is a question now at issue, and the basis for Alice's opinion becomes more important).

Expert evidence is also sometimes admissible, in circumstances where the expert offers an opinion on a matter on which people of ordinary background would be unlikely to form a correct judgment without aid. It might be necessary, for example, to use a properly-qualified expert to determine, definitively, whether Bob was building a bomb, as opposed to a souped-up pressure cooker. But even so, not every expert opinion has the same weight. The expert who examined Bob's contraption is in a very different position than the expert who based their opinion on a second-hand description of a device they have never seen.

If there is doubt about the factual foundation of an expert's opinion, that too reduces its evidentiary weight. For example, if the expert opines that Bob had the technical ability to make a bomb, it would matter whether this opinion stems from Yves's out-of-court statements that he and Bob attended the Acme bomb-making camp and Bob was the best in the class. The expert opinion is built on a fact that is itself the product of hearsay. This means that the trier of fact may be obliged to give the opinion no

weight because it has no factual foundation in the laws of evidence. And even if the expert's opinion survives because there are other, provable facts upon which it is based, the expert's opinion cannot be offered as proof that Bob did attend the Acme bomb-making camp.

III. DEFINING "INTELLIGENCE"

If evidence is information that is legally cognizable under the rules of evidence, what is "intelligence"? Definitions here are more difficult because there is no consensus understanding of the term. "Intelligence" may mean different things to different agencies, because their mandates may drive what it is they collect. CSIS, for example, mainly collects "security intelligence"; that is, intelligence relating to "threats to the security of Canada" as that expression is defined in the CSIS Act.[15] But, under different circumstances, it may also collect "foreign intelligence": "information or intelligence relating to the capabilities, intentions or activities" or foreigners or foreign states or entities.[16] A similar concept is found in the *Communications Security Establishment Act* (currently part of Bill C-59): "foreign intelligence means information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security."[17] Of course, this definition does not actually define "intelligence" (and strangely, juxtaposes it with "information"). Nor does it provide precision on what "relating" to international affairs, defence or security (all themselves ambiguous concepts) means.

At a collection level, "intelligence" is also often divided into different "intelligence disciplines,"[18] according to the source of the information. For instance, intelligence collected from human sources is "human intelligence," or HUMINT, while intelligence collected through interception of electronic communications is "signals intelligence," or SIGINT. There are still other ways intelligence could be divided, by source. Intelligence could be the product of direct observation (a CSIS employee

---

15 CSIS Act, *supra* note 6, ss 2, 12.

16 *Ibid*, s 16.

17 *Communications Security Establishment Act*, s 2, being Part III of Bill C-59, *An Act respecting national security matters*, 1st Sess, 42nd Parl, 2017 (first reading 20 June 2017).

18 Robert Clark, "Perspectives on Intelligence Collection," (2013) 20:2 J US Intelligence Studies 47.

sees Bob buy a pressure cooker at Walmart) or of intrusive surveillance (CSIS searches Bob's house, and bomb-making equipment is found). Intelligence could come from an informant who has, almost certainly, been offered anonymity and protection against the disclosure of his or her identity (CSIS confidential informant Alice hears Bob say "I am building a bomb"). It may also be shared intelligence, received from a foreign partner and likely "caveated" in a manner that limits its subsequent use by the recipient agency (The CIA tells CSIS that it believes Bob is building a bomb, which CSIS may use for investigative purposes but must not share). And it may also be packaged as processed analytical intelligence, compiling intelligence from any of the sources above (CSIS prepares an intelligence assessment from all the sources above, concluding Bob is building a bomb).

Still, at best, these sorts of classifications compartmentalize "intelligence" without defining it. And so, I shall also employ a generic understanding of intelligence:

> Intelligence is the umbrella term referring to the range of activities – from planning and information collection to the analysis and dissemination – conducted in secret and aimed at maintaining or enhancing relative security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation of a preventive policy or strategy, including, where desirable, covert activities.[19]

Under this reasoning, intelligence is all the information that contributes to these objectives. Intelligence is information collected, analyzed, assessed, shared and assigned a value directed at some intelligence objective. Intelligence will, therefore, have its own concept of materiality and relevance – it cannot serve its purposes without focusing on information that assists in proving the existence (or not) of facts that contribute to the objectives of intelligence.

But because the breadth of these objectives is expansive, and not tied to a choreographed legal proceeding, the standards of relevance and materiality are almost certainly more relaxed for intelligence than for evidence. Intelligence is designed to serve a predictive function tied to an ill-defined understanding of "security." This means the potential paths by which a given piece of information may prove relevant to a material fact are more plentiful than they are in a legal proceeding built around shared (or at least resolvable) understandings of the limited key issues in dispute.

---

[19] Peter Gill & Mark Phythian, *Intelligence in an Insecure World* (Cambridge: Polity Press, 2012) at 19.

As with evidence, intelligence practices may include their own heuristics – that is, shortcuts and protocols that, based on experience, maximize the chance of accuracy. Intelligence assessments will worry about the provenance, reliability and credibility of information. For example, an intelligence agency might regard as less reliable information from a single source that cannot be validated with other information. These practices may narrow the band of information processed as intelligence, by enabling more careful ingestion and evaluation of information. Understandings between agencies may also limit how intelligence is used. For example, "caveats" on intelligence shared between agencies may purport to limit how given intelligence in then used by the recipient service. And law itself may superimpose limitations for policy reasons on what information can be considered intelligence. For example, Canadian government policy limits the use to which information shared by foreign intelligence service may be put, where it is believed to be the product of mistreatment.[20]

But intelligence is not burdened to the same degree with the strict rules of admissibility that are part of the law of evidence. A hearsay exclusion would be nonsense to an intelligence practitioner, although that same analyst would still be worried about the credibility of the source.

Put another way, intelligence and evidence inhabit different worlds, and the broader, more diffuse concept of "intelligence" can sit poorly with the stricter, more technical concept of "evidence." As the Ontario Court of Appeal noted, discussing intelligence supplied by foreign services:

> [t]he source of the evidence is unknown. The circumstances in which the evidence was gathered are unknown. Often, the intelligence evidence itself is unknown because, for national security reasons, the named person is denied access to it. In the appellant's words, the intelligence information is "unsourced, uncircumstanced, and unknown."[21]

This decision concerned evidence supplied by France in a Canadian extradition proceeding. Despite these shortcomings, the Court of Appeal declined to rule intelligence inherently inadmissible. Rather, admissibility depended on whether the use of the intelligence would deny the "person's fundamental right to make answer and defence and have the benefit of a

---

20 See e.g. *Ministerial Direction to the Canadian Security Intelligence Service: Avoiding Complicity in Mistreatment by Foreign Entities* (25 September 2017), online: <www.publicsafety.gc.ca/cnt/trnsprnc/ns-trnsprnc/mnstrl-drctn-csis-scrs-en.aspx> [perma.cc/7U9P-52SK] [Ministerial Direction].

21 *France v Diab*, 2014 ONCA 374 at para 205.

fair trial."[22] In sum, the worlds of intelligence and evidence overlap, but not always in predictable manners.

IV. Defining "Intelligence-to-Evidence"

We reach, therefore, the question of "intelligence-to-evidence." Again, definitions matter, and here I offer my own. Intelligence-to-evidence is the inelegant phrase we use to describe several discrete types of issues. The first – at issue in the *Ahmad* matter noted in the introduction – is the movement of intelligence procured by intelligence services to support law enforcement, typically the police. I will call this the actionable-intelligence issue. An example would be CSIS supplying RCMP with the intelligence that Bob is building a bomb.

Ample actionable-intelligence is an ingredient of successful security – a point made in the 1985 Air India bombing inquiry,[23] by the 9/11 commission[24] and affirmed in the UK context by David Anderson's study of security services' performance in relation to the 2017 terror attacks in that country.[25]

In theory, police or other enforcement agencies could act on actionable-intelligence without worrying about how it dovetails with the concept of evidence. In practice, however, law enforcement agencies depend on legal proceeding. To perform their mission, they are not free to discard the conventions of evidence, at least not without running the risk of their conduct then being invalidated in one form or another. Likewise, intelligence agencies must contemplate how police – in their more legalized environment – will be obliged to use – and especially, disclose – the information intelligence services provide. The distance between intelligence and evidence matters, therefore, in considering even actionable-intelligence.

For this reason, actionable-intelligence sharing cannot be delinked from a second, closely-related component of I2E: something that I shall call the

---

22 *Ibid* at para 209.

23 See Air India Inquiry Vol 1, *supra* note 4; Roach, *supra* note 4.

24 National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: Norton, 2004) at 417.

25 David Anderson, *Attacks in London and Manchester March-June 2017, Independent Assessment of MI5 and Police Internal Reviews* (December 2017), online (pdf): <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf> [perma.cc/9UM5-S84R].

evidentiary-intelligence issue. Evidentiary-intelligence has two aspects. This first I will call the evidentiary-intelligence sword. The second, much better-canvassed issue in Canada is the evidentiary-intelligence shield problem.

The evidentiary-intelligence sword issue involves the use of intelligence in legal proceedings, to justify state action. For example, the prosecutor may wish to use intelligence provided by CSIS to RCMP to prove that Bob was planning to build a bomb. At issue, here, is the use of intelligence as evidence in a legal proceeding, either to justify police conduct or prevail in a legal dispute. Here, authorities must worry about the quality of the information, measured against the standards of evidence.

In comparison, the evidentiary-intelligence shield is about protecting intelligence from disclosure as part of a legal proceeding. For example, the government seeks to protect CSIS intelligence about Bob from disclosure to the defence, in a prosecution of Bob for building a bomb. As I argue below, while actionable-intelligence comes first in time, its scope will inevitably depend on an assessment of evidentiary-intelligence issues, especially shields. This preoccupation with evidentiary-intelligence is especially acute in the criminal law context. CSIS is determined that its "crown jewels"[26] – its targets, means, methods and sources – not be revealed in open court, dragged into a proceeding by Canada's broad criminal disclosure rules.[27]

The latter concern is a product of the Supreme Court's 1991 decision, *Stinchcombe*.[28]

A. "First Party" Disclosure Under *Stinchcombe*

In *Stinchcombe*, the Supreme Court found a general duty on the Crown to disclose all relevant information to the defence in a criminal case. The "Crown" is, in practice, prosecutors and the police, so-called "first parties" to the case. The Crown must disclose upon request from the defence,

---

26 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 *Final Report*, vol 3 (The Relationship Between Intelligence and Evidence) (Ottawa: Public Works and Government Services Canada, 2010) at 195, online (pdf): <epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air_india/2010-07-23/www.majorcomm.ca/en/reports/finalreport/volume3/volume3.pdf>.

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

28 *R v Stinchcombe*, [1991] 3 SCR 326, [1991] SCJ No 83.

without judicial intervention.[29] When prosecutors determine whether to disclose (or not) information in the possession of the Crown, nothing turns on admissibility, or whether the information is exculpatory or inculpatory, or whether the Crown intends to use the information as evidence or not, or whether it find the information credible or not: the disclosure threshold is "relevance."[30] The Crown has a disclosure obligation "whenever there is a reasonable possibility of the information being useful to the accused in making full answer and defence" [31] – that is, "in meeting the case for the Crown, advancing a defence or otherwise in making a decision which may affect the conduct of the defence such as, for example, whether to call evidence."[32] For instance, if the night-watchman who discovered Bob building a bomb called the police, the information stemming from the police interview with the night-watchman would be relevant to the material question of "was Bob building a bomb."

Stinchcombe prescribes a low threshold, and where it is resisted, the Crown bears the burden of justification. But there are limits to *Stinchcombe*. The implicit expectation in *Stinchcombe* is that Crown and police have information for criminal law purposes, and therefore their information holdings are likely relevant and that they comprise the case against the accused.[33] But this may not always be true, and *Stinchcombe* does not obliged disclosure of <u>every</u> possible piece of information in the police/Crown's possession relating to the case. The Crown and police have no obligation to disclose information that is "clearly irrelevant." As the Supreme Court has said, "[t]here is no constitutional right to adduce irrelevant or immaterial evidence."[34] The aperture of relevance – its scope – depends on what is charged, and any reasonable possible defences to these charges.[35] It is not

---

29 *R v Gubbins*, 2018 SCC 44 at para 19 [*Gubbins*].

30 *R v Illes*, 2008 SCC 57 at para 63.

31 *R v Dixon*, [1998] 1 SCR 244 at para 21, [1998] SCJ No 17.

32 *R v Egger*, [1993] 2 SCR 451 at para 20, [1993] SCJ No 66.

33 *R v McNeil*, 2009 SCC 3 at para 20 [*McNeil*].

34 *R v Pires*; *R v Lising*, 2005 SCC 66 at para 3.

35 *R v Taillefer; R v Duguay*, 2003 SCC 70 at para 59. For instance, relevance is levered open where entrapment is a plausible defence. In *Nuttall*, the defence argued entrapment, after the police commenced a criminal investigation into the accused without reasonable suspicion of criminal activity and then induced criminal conduct. The court concluded the shared CSIS information that initiated the police investigation was relevant to this defence, and subject to *Stinchcombe*. *R v Nuttall*, 2015 BCSC 1125 [*Nuttall*].

relevant, for example, that the night-watchman was an Afghanistan veteran and that he had coffee during the interview with the police. There is no reasonable likelihood this information affects the probability that Bob built a bomb. (On the other hand, if the police knew that Bob used to beat up the night-watchman in high school, this is relevant to the question of whether the night-watchman might be lying, a matter that clearly affects the likelihood of whether the night-watchman saw Bob build a bomb.)

Nor does the Crown have an obligation to disclose so-called "background information" or "operational records" not specific to any particular investigation. Such information includes, for example, the maintenance records concerning a piece of technology used in an investigation.[36]

B. "Third Party" Disclosure Under *O'Connor*

The *Stinchcombe* disclosure obligation is on the Crown. It does not extend directly to the information holdings of other government agencies – so-called "third parties." And so CSIS has been treated as a "third party," at least so long as its investigation is not so interwoven with that of the police that courts regard the two as conflated and organized with the purpose of charging and prosecution.[37] This does not mean that a government third party (in this case, CSIS) has no disclosure obligations. Moreover, the Crown does have an obligation to make reasonable inquiries of third-party state agencies that may be in possession of relevant information.[38] But the third-party disclosure standard is different from *Stinchcombe*. Instead, it is governed by the *O'Connor* approach.[39] The *O'Connor* approach does set a higher threshold on disclosure to the defence than does *Stinchcombe*: one of "likely relevance"[40] (rather than "not clearly irrelevant"). This *O'Connor* threshold is "significant, but not onerous,"[41] and excludes "fishing

---

36 *Gubbins*, *supra* note 29.

37 See e.g. *R v Ahmad*, *supra* note 1.

38 *McNeil*, *supra* note 33 at para 13.

39 *R v O'Connor*, [1995] 4 SCR 411, [1995] SCJ No 98 [*O'Connor*]. See e.g. *Nuttall*, *supra* note 35 for recent applications of this test to CSIS.

40 *O'Connor*, *supra* note 39 at para 22. For a recent case applying *O'Connor* to CSIS, see *R v Peshdary*, 2017 ONSC 1225.

41 *Gubbins*, *supra* note 29 at para 26; *O'Connor*, *supra* note 39 at paras 24, 32. See also *Gubbins*, *supra* note 29 at para 27 ("Likely relevance" is a lower threshold than "true relevance", and has a "wide and generous connotation").

expeditions" for "irrelevant evidence."[42] But *O'Connor* differs most dramatically from *Stinchcombe* in creating a judicial gate-keeper to disclosure: Under *O'Connor*, the defence must persuade a court to order disclosure.

In a first step under the *O'Connor* process, the accused must persuade a trial judge that "there is a reasonable possibility that the information is logically probative [that is, tending to prove] to an issue at trial or the competence of a witness to testify."[43] Or, put another way, the defendant must show that the information is relevant to a material issue at trial. Issues at trial include not only "material issues concerning the unfolding of the events which form the subject matter of the proceedings, but also 'evidence relating to the credibility of witnesses and to the reliability of other evidence in the case.'"[44]

For example: If the night-watchman is the Crown's witness in Bob's prosecution, the defence will likely want to know what the night-watchman might have said to CSIS, as part of CSIS's separate investigation into the bomb plot. The defence will need to persuade the trial court that there is a reasonable possibility that these CSIS interview notes constitute information logically probative (that is, they tend to prove) the merits of the night-watchman's testimony. There is a good chance of success on this point.

And if the defence succeeds, then the judge will order production of the information for the judge's own review. In this second stage, the judge weighs the different considerations favouring disclosure or non-disclosure to the accused. The caselaw does not propose a closed list of considerations guiding this assessment. In keeping with *O'Connor*'s specific facts, courts have emphasized fair trial considerations versus personal privacy interests in, especially, medical or psychiatric records. And so, if the CSIS interview included a psychiatric assessment of the night-watchman, the court would need to weigh the fair trial virtues of disclosing this assessment against the privacy interests of the night-watchman. But it seems unlikely that a simple interview between the informant and a CSIS officer would raise acute

---

42 *McNeil*, *supra* note 33 at para 28.

43 *O'Connor, supra* note 39 at para 22.

44 *McNeil*, *supra* note 33 at para 33. There are caveats on this point. For one thing, the lower court caselaw suggests that a court may be attentive to redundancy, and decline to review documents containing information already in the hands of the defence. See e.g. *R v Nicholson*, 2016 BCSC 1831 at para 33; *R v Batte*, (2000) OR (3d) 321, 2000 CanLII 5751 (Ont CA) at para 75.

privacy interests of this nature. And what other considerations would go into this disclosure/nondisclosure balancing in a CSIS case are not prescribed: there is no legislative guidance here, as there has been in other contexts.[45] For reasons discussed below, I doubt the second prong of the *O'Connor* test could ever be very protective of CSIS secrets, whether legislated or not.

At any rate, the caselaw on CSIS secrets on the *O'Connor* approach is not especially helpful. Most of what can be usefully extracted from it concerns the first prong of the *O'Connor* test. For instance, in a case where the defence sought the entire CSIS investigatory information holding, the court noted that CSIS's mandate "is significantly different than that of the RCMP" and where the case is built entirely on information collected by the police, the defence fails "to show the likely relevance of the CSIS investigation as a whole to the issues" at trial.[46] That is, the aperture of relevance does not reach an entire CSIS investigation, just because it too was investigating the same target.

On the other hand, where the issue at trial is an entrapment defence, and at issue is whether a person was a CSIS source being directed by CSIS, production may be ordered, even at risk of impairing source identity.[47] And so, if Bob's claim is that he was entrapped into working on the bomb by the state, the court may order disclosure of information on the CSIS IO's conduct, even at risk of revealing Alice's identity as the IO's confidential informant. (And this development would likely spark a CSIS supplemental blocking effort, under the privileges discussed below.)

C. Wiretaps and Disclosure

Different disclosure issues arise where a prosecution is supported by the fruits of a wiretap (or possibly, other forms of search warrant). Except in exigent circumstances, a police wiretap is authorized by a form of warrant, issued after a closed-door (*in camera*) judicial proceeding in which only the government side appears (*ex parte*). Police applications must be supported by evidence. Most notably, they must include an affidavit in which police affiants spells out the facts for their "reasonable grounds to believe" that interception of specified people's communications may assist in the

---

45 See *Criminal Code*, RSC, 1985, c C-46, s 278.1ff, relating to third-party records containing the personal information of a complainant or witness [*Criminal Code*].

46 *R v Peshdary*, 2018 ONSC 1358 at para 43 [*Peshdary, ONSC*].

47 *R v Nuttall*, 2016 BCSC 154 at paras 9-11.

investigation of an offence.[48] The rules of evidence for such warrant affidavits are relaxed: they may include hearsay.[49]

Because the constitutionality of a wiretap depends on it meeting the strict requirements in the *Criminal Code*,[50] a defendant later prosecuted because of evidence stemming from the wiretap may wish to challenge the admissibility of that evidence by showing that the warrant was unlawfully issued (or used). This is done in what is known as a *Garofoli* challenge.[51] Here, the later judge retrospectively reviews the validity of the warrant issued by the earlier, authorizing judge.

The material issues in a *Garofoli* matter are, only, whether the record before the original, warrant-authorizing judge satisfied the statutory preconditions for the warrant, and whether that record accurately reflected what the affiant knew or ought to have known. And if the record does not meet this standard, the question then is: were the errors egregious enough to affect the issuance of the warrant.[52] The reviewing judge will invalidate the warrant where, upon review of the material before the authorizing judge, the reviewing judge believes there was "no basis upon which the authorizing judge could be satisfied that the preconditions for the granting of the authorization existed."[53]

To conduct this probe, the reviewing judge and the parties must obviously have access to the materials originally before the authorizing judge. For a police warrant, the information undergirding a warrant may already be part of the police investigative file, already disclosable to the

---

48 *Criminal Code*, *supra* note 45, s 185(1). Sometimes called "reasonable and probable grounds" in the constitutional caselaw, "reasonable grounds to believe" is much lower than the criminal trial standard of "beyond a reasonable doubt." Instead, it is defined as a "credibly-based probability" or "reasonable probability." *R v Debot*, [1989] 2 SCR 1140, [1989] SCJ No 118.

49 See *Eccles v Bourque*, [1975] 2 SCR 739 at 746 ("That this information was hearsay does not exclude it from establishing probable cause," in an arrest context); *R v Morris*, 1998 NSCA 229, (1999), 134 CCC (3d) 539 at 549 (NS CA) ("Hearsay statements of an informant can provide reasonable and probable grounds to justify a search."); *R v Philpott*, 2002 CanLII 25164 (Ont Sup Ct J) at para 40, 56 WCB (2d) 163 ("The [warrant] issuing court may consider hearsay evidence obtained by the affiant from other officers or informants.").

50 See discussion on this point in *Huang*, *supra* note 27 at para 14.

51 *R v Garofoli*, [1990] 2 SCR 1421, [1990] SCJ No 115.

52 See *World Bank Group v Wallace*, 2016 SCC 15 at para 120 [*Wallace*].

53 *R v Pires*; *R v Lising*, *supra* note 34 at para. 7.

defence under *Stinchcombe*'s broad relevance test. Here, the *Garofoli* challenge does not broaden the aperture of disclosure.

But if not all the supporting information related to the warrant has been disclosed as relevant to the trial under *Stinchcombe*, then it is potentially disclosable under this new challenge, because it has introduced new, material issues. In a *Garofoli* challenge, the affidavit supporting the warrant authorization and the documents before the authorizing judge are presumptively disclosable.[54] But beyond that, there are limits: relevance applied in a *Garofoli* context does not authorize a fishing expedition through documents never before the affiant whose affidavit supported the warrant application, in part because the courts have been sensitive about revealing confidential sources.[55] And so, for documents further afield than the affidavit and the documents it relied on, it is for the accused to "establish some basis for believing that there is a reasonable possibility that disclosure will be of assistance on the application" to challenge the warrant.[56] This is not easy to do. Applying this standard, lower courts have found instances where some police information – for example, notes kept by the handler of a confidential informant – are irrelevant both for the trial and for testing a search warrant.[57]

Warrant disclosure issues become even more complicated where at issue is a CSIS warrant. CSIS can collect intelligence through wiretaps under its own, separate CSIS Act warrant procedures, involving authorizations by the Federal Court. Here, the warrant application is supported by a CSIS affidavit asserting the facts believed, on reasonable grounds, to show why the warrant would enable CSIS to investigate a threat to the security of Canada.[58] Sometimes CSIS will then find things that are important for the police to know. That is, sometimes CSIS discovers actionable-intelligence. In a functioning intelligence-to-evidence system, CSIS will share this actionable-intelligence in an advisory letter; that is, a letter from CSIS to the RCMP containing intelligence and permitting its use in legal

---

54 *Wallace*, *supra* note 52 at para 134.

55 *Ibid* at para 129ff.

56 *R v Ahmed*, 2012 ONSC 4893 at paras 30-31, an approach cited without objection in *Wallace*, *supra* note 52 at para 131.

57 See e.g. *R v Ali*, 2013 ONSC 2629, cited without objection in *Wallace*, *supra* note 52 at para 131.

58 *CSIS Act*, *supra* note 6, s 21.

proceedings.[59] And the CSIS information then finds its way into the police investigative, one that may culminate in charges and a prosecution.

In consequence, CSIS may worry that the contents of its wiretap intercept (or other search), used to further an RCMP investigation, might later attract *Garofoli*-style scrutiny of CSIS's own Federal Court authorization and the basis for it.[60] Since that CSIS warrant may be built on confidential source information, foreign origin intelligence and signals intelligence, it would not wish too close an inquiry in open-court into the evidence undergirding the Federal Court warrant.

The likelihood of a CSIS warrant *Garofoli* challenge is greatest should the information collected by CSIS be presented in evidence as partial proof of crimes charged.[61] If the CSIS warrant was invalid, then the information flowing from it would be excluded from the trial. And therefore, defence lawyers would have a direct incentive to test the CSIS warrant. But the more likely scenario is this: the shared CSIS intelligence is one of the pieces of evidence police used to obtain their own wiretap. This police wiretap then produces evidence used in the trial.

Put another way, the CSIS warrant is two steps removed from the evidence used in the trial. Even so, CSIS's warranted intercept activity must stand up in the criminal court, where it is the foundation of a criminal investigation. This is true even if the information shared by CSIS in an advisory letter is not used as direct evidence of a crime in trial, but simply as evidence by police supporting the reasonable grounds to believe required to obtain a *Criminal Code* search warrant or authorization. If the defence lawyer can knock over the CSIS warrant, and information collected by the CSIS warrant was the basis for the police warrant, the dominos fall.

Again, the scope of relevance in this two-steps-removed *Garafoli* context would be tied to the narrow purpose of challenging the warrant. But to add to the complexity, CSIS is likely a "third party," not the Crown. And where

---

59 An "advisory letter" "contains information that may be used by the RCMP to obtain search warrants, authorizations for electronic surveillance or otherwise used in court. In the case of Advisory letters CSIS requires the opportunity to review any applications for judicial authorizations prior to filing." CSIS-RCMP Framework for Cooperation, One Vision 2.0 (10 November 2015) at 2, posted at *Secret Law Gazette*, online: <secretlaw.omeka.net/items/show/21> [perma.cc/9XHZ-KEBD] [One Vision 2.0].

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

61 This is indeed happening in the Huang prosecution. See discussion in Huang, supra note 27 at para 9.

CSIS has *O'Connor* third-party status, disclosure of information relevant to this purpose will follow the *O'Connor* two-step process: first, the defence will need to show the "likely relevance" of the documents being sought; second, if they do so, the documents are reviewed *in camera* and *ex parte* by the judge.[62]

In practice, application of this test has meant that (at least redacted) copies of the CSIS affidavit supporting the CSIS warrant will be disclosed, along with any supporting material actually before the warrant-authorizing judge.[63] Courts may also oblige disclosure of draft warrant applications.[64] There is also the possibility the CSIS affiant may be cross-examined, but only with leave of the court and confined to the question of whether the affiant knew or ought to have known about errors or omissions in the warrant application.[65] It is unlikely source materials undergirding the warrant documents must also be disclosed – where CSIS is a third party under the *O'Connor* rule, lower courts have required the defence to show that "there is a factual basis for believing that the material sought will produce evidence tending to discredit a material pre-condition in the CSIS Act authorization."[66]

D. Privilege and Immunities

It is also important to note that neither *Stinchcombe* nor *O'Connor* annul privileges in the law of evidence, including police informer identity

---

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

63 *Jaser*, *supra* note 62 at para 18 (observing that the "CSIS Affidavit on which the Federal Court authorization depends easily meets the first stage O'Connor/McNeil test of 'likely relevance'"); *R v Alizadeh*, 2013 ONSC 5417. The test is whether the documents will be of probative value on the issues in the application – that is, the validity of the warrant. More specifically: "would the justice have had reason to be concerned about issuing the warrant had he or she been made aware of the other facts". *R v Peshdary*, 2018 ONSC 2487 at para 9ff.

64 *R v Peshdary, ONSC*, *supra* note 46.

65 *R v Pires*; *R v Lising*, *supra* note 34 at para 40ff. See also *World Bank*, *supra* note 52 at para 121ff.

66 *Peshdary, ONSC*, *supra* note 46 at para 20. See also *Peshdary, FC*, *supra* note 60.

privilege[67] and the new CSIS informer privilege.[68] Moreover, disclosure obligations are subject to a national security public interest immunity codified in s. 38 of the *Canada Evidence Act*. Section 38 is a form of evidentiary intelligence shield, allowing the government to block disclosure of sensitive information.

Under s. 38, specially designated Federal Court judges decide whether the information in question is relevant to the underlying proceeding. Where the disclosure dispute is tied to a *Criminal Code* trial, "relevance" in a criminal context is the *Stinchcombe* test.[69] But still, relevance depends on the context. For instance, relevance will be narrower when the issue is the validity of a warrant in a *Garofoli* proceeding than if the issue is evidence in the criminal trial itself.[70] Moreover, CSIS warrants tied to a broad threat investigation may include information unrelated to the intercept of a specific target's telephone call. This extraneous information may not be relevant to that person's subsequent *Garofoli* challenge.[71]

Then, if the information is relevant, the judge decides whether the material, if disclosed to the accused, would harm national security, national defence, or international relations. If it would, the judge then balances this injury against the public interest in disclosure. If the security interest exceeds the public interest (often, but not exclusively, in the form of the defendant's right to make full answer and defence),[72] the judge will protect the information from disclosure or may order the information disclosed only in redacted or summarized form.

Even if the Federal Court orders information disclosed, the government has, essentially, an absolute ability to stop disclosure under s. 38, using what is known as an "Attorney-General's certificate." This certificate allows the government to short-circuit a court disclosure order. Section 38.13 of the Act empowers the Attorney General (AG) to personally issue a certificate "in connection with a proceeding for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity as defined in

---

67 *R v Leipert*, [1997] 1 SCR 281 at para 21, [1997] SCJ No 14. That privilege has an outer limit. It does not apply to identity information that goes to the very question of innocence or guilt: where there is "a basis on the evidence for concluding that disclosure of the informer's identity is necessary to demonstrate the innocence of the accused".

68 CSIS Act, *supra* note 6, s 18.1

69 *Huang* FCA, *supra* note 62 at para 23.

70 *Ibid* at para 14.

71 *Huang*, *supra* note 27 at paras 50, 59.

72 *Ibid* at paras 50-52.

subsection 2(1) of the *Security of Information Act* or for the purpose of protecting national defence or national security."

Issuance of the certificate has the effect of barring any subsequent disclosure of the information in a proceeding for ten years (and for a further period if the certificate is renewed at the end of that ten years). In other words, the certificate may reverse an order from the Federal Court authorizing disclosure under s. 38, subject to a very narrow and limited appeal before a single judge of the Federal Court of Appeal.

The AG Certificate is an emergency rip-cord. As Justice Canada counsel Don Piragoff told the Senate when the provision was enacted:

> The provision is a last resort for the Attorney General to ensure that information critical to national security is not disclosed in judicial proceedings to which the Canada Evidence Act applies or through other government processes. ...The certificate issued by the Attorney General...would be the ultimate guarantee that information such as sources of information and names of informers would not be made public.[73]

Based on conversations with government officials, I believe the AG certificate has never been used since the creation of this power in 2001.

Protecting information using s. 38 comes with a cost. For one thing, the s. 38 process can be unwieldy. The disclosure decisions made by the Federal Court are generally made before the terrorism trial starts, and the process can be long and fraught. Moreover, the prosecution cannot use the information shielded under s. 38. That is, information shielded cannot be used as a sword in a prosecution.

Even more dramatically: if the Federal Court (or Attorney-General certificate) denies disclosure of information on security grounds that is important to the defence, there will doubts about the fairness of the trial. This may scuttle trials. A trial judge accepts whatever non-disclosure decision the Federal Court makes. But the trial judge also must make a difficult decision on whether to halt the prosecution because the Federal Court's non-disclosure order has made the trial unfair. And he or she might need to do so without even knowing the specifics of the secret information.[74]

---

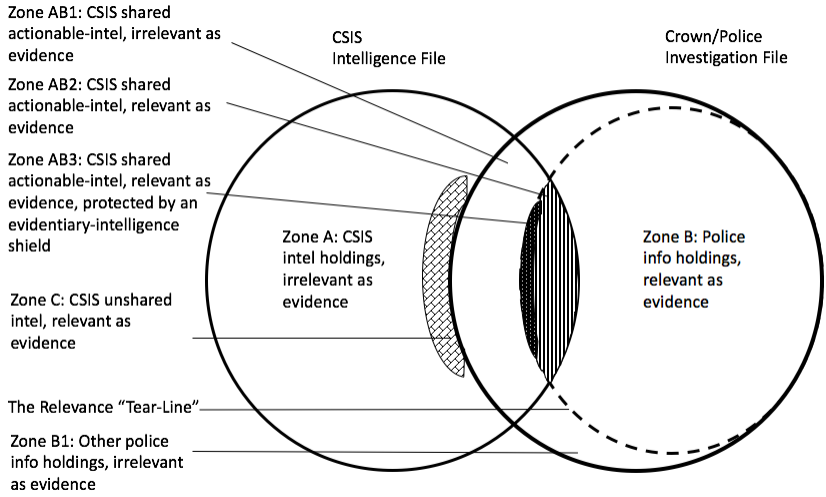
73 Senate, Special Senate Committee on the Subject Matter of Bill C-36, *Issue 1 - Evidence*, 37-1, (22 October 2001), online: <sencanada.ca/en/Content/Sen/committee/371/sm36/01evb-e> [perma.cc/5H6M-27KM].

74 In *R v Ahmad*, 2011 SCC 6 [*Ahmad* SCC], the Supreme Court recognized that the two-court s. 38 system could "cause delays and pose serious challenges to the fair and expeditious trial of an accused, especially when the trial is by jury" (para 76) but decided

E. Consequences

The net result of all these evidentiary-intelligence issues is a taxing and incredibly uncertain system that greatly complicates actionable-intelligence sharing as CSIS and the police engage in an arcane choreography to minimize disclosure of sensitive CSIS intelligence. In figure 1, I present a pictorial image of how different information categories overlap in a police and intelligence investigation.

Figure 1: Possible Intelligence-to-Evidence Zones



The rules of evidence overlap with these zones in the manner portrayed in table 1.

---

that it was constitutional because the trial judge could always stop a trial, should the Federal Court's non-disclosure order make it impossible for the accused to have a fair trial. The Court stressed that "the trial judge may have no choice but to enter a stay." *Ibid* at para 34. Some participants in the case argued that this approach "puts the Attorney General and the trial courts in the dilemma of playing *constitutional chicken*" (para 34). For its part, the Court expressed the hope that a sensible application of s. 38 would avoid such a result, perhaps using the intermediary of a security-cleared special advocate as a link between Federal and trial courts.

Table 1: Topology of I2E

Zone	Initial Disclosure Standard	Evidentiary-Intelligence Shield (Public Interest Immunities)
A	Not disclosable under any standard, because irrelevant.	N/A
B	Disclosable under *Stinchcombe*, because relevant and in possession of police investigators.	Source identity information may be protected under police source identity privilege. Other public interest privileges in the *Canada Evidence Act*, could apply, including s. 38, requiring a proceeding in the Federal Court.
B1	Not disclosable under any standard, because irrelevant.	N/A
AB1	Not disclosable under any standard, because irrelevant.	N/A
AB2	Disclosable under *Stinchcombe*, because relevant and in possession of police investigators.	N/A (the chart assumes that the information over which CSIS claims privilege is in AB3.)
AB3	Disclosable under *Stinchcombe*, because relevant and in possession of police investigators.	In this zone, protected under, e.g. CSIS source identity protections or under *Canada Evidence Act* s. 38 (the national security imperative outweighs the public interest as assessed by the Federal Court, or the Attorney General issues a certificate denying disclosure after a Federal Court disclosure order.)

C	Disclosable under *O'Connor*, if CSIS has third-party status: the defendant must show the likely relevance of this information, and the trial court must then review and weigh the disclosure interest against the non-disclosure interest.	Should the court order disclosure, the Crown could still seek to protect this information under privileges, such as those listed above under AB3.

It may not always be clear at the outset of a case into which zone information falls. Moreover, the core structural problem with this complicated architecture is this: I2E dilemmas limit the size of the AB zones – that is, the zones in which CSIS shares actionable-intelligence. CSIS will fear that its shared intelligence will fall on the *Stinchcombe* disclosure side of the "relevance tear-line," into zone AB2. It may find the tear-line boundary between irrelevant (AB1) and relevant information (AB2) difficult to predict in advance. CSIS may subsequently protect some of the information in AB2 through the *Canada Evidence Act*, s. 38, creating zone AB3. This evidentiary-intelligence shield risks scuttling a prosecution, if AB3 information is necessary for a fair trial (or to secure a conviction). And so, police themselves may be wary of building a case on shared CSIS zone AB information that the government would then seek to protect under s. 38 (that is, it will end up being AB3 information). Moreover, since the outcome of the s. 38 process cannot be predicted in advance, CSIS may err on the side of under-disclosure to the police, creating zone C. This may be a pyrrhic victory. It would deprive police of potentially important actionable-intelligence. At the same time, it would not shield CSIS completely from disclosure risk: the information will still be subject to *O'Connor* disclosure procedures, and that in turn may spark recourse to s. 38.[75]

The possible consequences of this suboptimal information management approach can be summarized as follows:

- Public Safety Risk: Siloed information holdings may not be pieced together to identify security risks. And information acquired for intelligence purposes by CSIS may not be shared seamlessly with

[75] See e.g. Canada (Attorney General) v Peshdary, 2018 FC 369.

police, legally empowered to act physically to diminish public safety risks.

- Investigative Inefficiency: Services may conduct duplicative investigations, expending scarce resources to chase the same target. This will make investigations more expensive, especially where these parallel investigations persist simply to avoid I2E dilemmas. And the obvious opportunity cost is investigations that are not mounted for lack of resources.

- Investigative Timing and Latent Threats: I2E struggles may make it impossible to respond to latent threats. For instance, a CSIS investigation may produce evidence of a crime. But if the I2E strategy does not permit the use of that evidence to secure a conviction, prosecution of that crime will depend on evidence separately collected by police. If, however, the target discontinues their conduct prior to the commencement of the police investigation (perhaps aware of the CSIS interest), there is no evidence allowing a prosecution. The target escapes the criminal net, unless police are prepared to continue their investigation indefinitely in the hope the target will reengage (raising the resource issue anew). The matter may instead return to CSIS, risking a recurrence of the difficult I2E handover to RCMP should the target re-engage in criminal threat activities. Variations of this problem arise where the target's conduct took place overseas, and information on it stems from intelligence sources that cannot be used in court (for instance, foreign terrorist fighters returning from Iraq or Syria).

- De Facto Criminal Immunity: Absent very careful coordination, I2E struggles may "poison-pill" downstream prosecutions. For instance, a CSIS threat reduction measure undertaken without sufficient attentiveness to its impact on the evidentiary record, or how it might be treated in a prospective prosecution, may make it impossible to prosecute. The record may be muddled with CSIS activity, disclosure of which would be prejudicial. Or the threat reduction measure is of a sort that would be regarded as an abuse of process (for instance, entrapment), and thus make a conviction

> impossible. Alternatively, defence counsel aware of I2E dilemmas may press for disclosure as a form of "graymail"; that is, forcing government to withdraw charges or risk disclosure of sensitive intelligence. In these circumstances, the target would enjoy *de facto* immunity from criminal process.

To explore how some of these outcomes might culminate in disastrous outcomes, I examine how Bob the Bomb-Builder first came to CSIS's attention.

V. The Plot

A. Genesis

It turns out Bob has a long history and a past tied to tragic events. Some time ago, he became a CSIS subject of investigation because of intelligence supplied by Jordan. The Jordanians shared metadata with CSIS suggesting Bob had been in regular communication with another Canadian believed to be in Syria, and associated with Hezbollah (a listed terrorist entity under Canada's *Criminal Code*) as a bomb-maker.

CSIS used this intelligence to start a security intelligence investigation into Bob. The Jordanian intelligence has regularly proven reliable and was deemed credible enough in its details to meet a legal threshold – "reasonable grounds to suspect" a threat to the security of Canada.[76] (If CSIS came to a different conclusion, it would have no jurisdiction to investigate – it should not even run a Google search on Bob.) Because there is not yet any legal proceeding, CSIS does not need to justify this decision in a proceeding governed by the rules of evidence.[77]

It is true that under ministerial directions that govern its conduct, CSIS must be wary of using information from a foreign partner that is likely to have been procured by maltreatment. Since this intelligence was metadata from a foreign wiretap, and not from a human source (who might have been maltreated), CSIS regards it as unlikely that the Jordanians obtained the information through mistreatment. At any rate, CSIS is not absolutely

---

76 CSIS Act, supra note 6, s 12. For a definition of how "reasonable grounds to suspect" is defined in law, see the text accompanying note 82.

77 It is possible that its expert review body – at the time of this writing, the Security Intelligence Review Committee – might subsequently review this investigation. But in conducting its review, SIRC would not hold CSIS to rules of evidence.

barred from using information stemming from mistreatment. Such information could not be used in a "judicial, administrative or other proceeding,"[78] even if CSIS wanted to. But initiating an investigation is not a "proceeding." Moreover, it does not itself create risk of further mistreatment or deprive anyone of their rights. And so CSIS could comply with ministerial direction and still rely on the Jordanian information.

As part of its investigation, Bob is tailed in Canada by a covert CSIS surveillance team. During this surveillance, Bob meets with another man, later identified as Yves. Yves is a foreign national and his precise involvement with Bob is unclear. At their meeting in a public café, a CSIS intelligence officer acting as part of the surveillance team hears Yves tell Bob about a meeting Yves is organizing for "those who believe like we do." This is all the information the officer overhears, although there is more to the conversation.

This is new intelligence. And again, it can be used to further an intelligence investigation without any concern about the rules of evidence.

B. A First Stab with CSIS's Evidentiary Sword?

CSIS would, of course, wish to know more about Bob, Yves, and their planned meeting. One way to do that might be to intercept their electronic communications, or search their premises. To make the step to intrusive surveillance or the searching of premises, CSIS would need to commence a legal proceeding. Under the *Charter of Rights and Freedoms*, Part VI of the *Criminal Code* and the CSIS Act, a wiretap of Bob and Yves's electronic communications requires a warrant.[79] Likewise, a search of premises in which either has a reasonable expectation of privacy – for instance, their homes – also requires a warrant.

CSIS investigators might, however, worry whether they would receive a warrant at this point of the investigation. A warrant requires using

---

78 See Ministerial Direction, *supra* note 20. This duplicates an existing legal requirement. Whether in raw or processed form, it is not possible to use as evidence in any proceeding over which Parliament has jurisdiction "any statement obtained as a result" of torture criminalized in s. 269.1 of the Criminal Code. Criminal Code, s 269.1(4). Such use would also violate the *Charter*, and would be the quintessential example of conduct violating fair trial rights (as well as Canada's international human rights obligations).

79 Intercept of private communication is protected under section 8 of the *Charter*. *R v Duarte*, [1990] 1 SCR 30 at paras 18-19, [1990] SCJ No 2. The authorization process for intercept for the police is found in *Criminal Code*, *supra* note 45, Part VI and for CSIS, in CSIS Act, *supra* note 6, s 21.

intelligence as evidence (that is, information that is probative of material legal issues), because it involves a proceeding in front of the Federal Court. This is a modest proceeding – it is done in secret, with only the government side represented. And the rules of evidence are relaxed. As with Criminal Code warrants, CSIS warrant applications may include hearsay, including intelligence-based allegations.[80] That means the Jordanian intelligence – clearly hearsay – would be admissible. So too, the CSIS officer's observations are direct evidence. Both sources constitute evidence of material facts used to decide whether a legal test in met. In this case, that test is whether there are "reasonable grounds to believe" the existence of a threat to the security of Canada, something that includes terrorism.

But at this point in the investigation, CSIS would be unwise to seek a warrant. While "reasonable grounds to believe" is a low threshold,[81] the evidence available to CSIS to meet even this threshold is weak. The Jordanian intelligence shows, at best, calls between Bob and a Canadian, who is believed (on bases that might be difficult to defend before an inquisitive judge without further details from the Jordanians) to be affiliated with Hezbollah as a bomb-maker.

And the CSIS officer's observations about a prospective meeting between the like-minded could be construed both innocently and less innocently. For example, it could involve a gathering of the small subset of people who enjoy *Saturday Night Fever*. And since the officer heard only a snippet, and not the full context, it could even be argued that what he or she heard is irrelevant under the law of evidence: it is so decontextualized it cannot be used one way or another to prove anything material to the proceeding. Relevance is always a standard in any legal proceeding. And the observed snippet of conversation is no more likely, as a matter of logic, to point to a threat to the security of Canada than is the fact that the two men spoke in low tones while drinking their white chocolate mochas.

---

80 For instance, the CSIS affidavit sworn as Federal Court file CSIS 15-12 (sworn in relation to Raed Jasser) specifies at para 6: "The information in this affidavit has been conveyed to me by employees of the Service who are, or were, involved in the Service's investigation of international Islamist terrorism and through a review of relevant records maintained by the Service. The information was obtained through various sources including government agencies, open information, as well as [redacted] associated with international Islamist terrorism." (The affidavit is supported by exhibits, fully redacted.) Likewise, the affidavit PPSC Number 1-12-073 (concerned Raed Jaser) relies on information conveyed in, e.g. letters from the FBI.

81 For a definition of this concept, see the text accompanying note 48.

Because a Federal Court judge would almost certainly toss a warrant application, CSIS continues its non-intrusive intelligence investigation. Days later, the CSIS surveillance units trail Bob and Yves to a residence in suburban Ottawa. They see another person, not known to CSIS, also enter the home.

C. Where are the Police?

So far, CSIS has not notified the RCMP. While the investigation of terrorism offences is within the RCMP's remit, there is precisely nothing at this point to suggest criminal conduct.

One response to this observation is: So what? An anti-terror intelligence investigation may come to naught, but if there is enough information to start such an investigation, the expectation must be that it could lead, in the fullness of time, to criminal charges. Canada's anti-terrorism laws are broad, and it does not take much to trip the line of criminal conduct. In these circumstances, while it may make sense to have CSIS lead such an investigation, it also makes sense to have RCMP in the wings, and fully apprised.

That is not likely to happen in my hypothetical, because Canada has not adopted a blended security intelligence/police approach to anti-terrorism. Part of the reason for this is institutional: two agencies with different mandates, approaches and histories. But the factor that holds these agencies apart is Canada's disclosure regime in criminal proceedings. CSIS is determined that its sources and methods not be revealed in open court, dragged into a proceeding by the *Stinchcombe* rule. A conflated CSIS/police investigation would mean CSIS was no longer a "third party." It would instead by fully subject to the *Stinchcombe* "not clearly relevant" disclosure standard, extended to the entire CSIS investigation. And so, in practice, police and CSIS maintain a carefully choreographed distance.

D. The Forger

The RCMP is, however, busy investigating (other) possible criminal activity. One of its targets of investigation is Trent. Trent came to the RCMP's attention while it was investigating drug trafficking by organized crime. Trent is suspected of forging Canadian passports (a crime) for use by organized crime syndicates. This suspicion does not, however, reach the level of reasonable and probable grounds for the RCMP to arrest Trent, let alone constitute enough for prosecutors to secure a conviction. Nor does

the RCMP have the "reasonable grounds to believe" required for a search warrant or wiretap.

It does, however, have enough evidence to meet the lower, "reasonable grounds to suspect" standard that can be used to obtain a transmission data tracking device for Trent's car.[82] With a tracking order in place, the RCMP follows Trent to a suburban Ottawa home. There, it also observes two other people – both unknown to the RCMP – enter the house.

E. The Signals Intelligence

Meanwhile, while collecting foreign intelligence on Hezbollah, the Communications Security Establishment (CSE) intercepts a mobile call between a Hezbollah field commander in Lebanon and Canadian Person (CP) A. In that call, the field commander suggests a "big, loud party in Canada that their government will never forget," and tells CP A "to gather the friends to begin the planning" and asks for a "new supply of papers."

CSE may not direct its intelligence activities at Canadians or persons in Canada,[83] but it does retain incidentally collected information of this sort that, as would be the case here, engages national security concerns. It also shares that intelligence with its domestic partners, initially in a manner that redacts information that would identify a Canadian (a process of "minimization"). These redactions can, however, be lifted administratively.[84] I assume intelligence of the sort implicating CP A would be shared with CSIS, and deminimized. CSIS then discovers that the identifying information in the CSE intercept matches that of Yves.

That means CSIS now has both Jordanian and CSE intelligence suggesting something is afoot in Canada. The CSE intelligence ties Yves to an ominous sounding Hezbollah-orchestrated "party" in Canada and a

---

82 *Criminal Code*, *supra* note 45, s 492.1 ("reasonable grounds to suspect that an offence has been or will be committed"). A lower standard than "believe on reasonable grounds," "suspects on reasonable grounds" is a suspicion based on objectively articulable grounds that may be lower in quantity or content than the requirement of reasonable belief, but must be more than a subjective hunch. *R v Kang-Brown*, 2008 SCC 18. Or put another way, "reasonable suspicion is a lower standard, as it engages the reasonable possibility, rather than probability, of crime." *R v Chehil*, 2013 SCC 49 at para 27

83 *National Defence Act*, RSC, 1985, c N-5, s 273.64.

84 For a discussion of aspects of this process, see Commissioner of the CSE, *Annual Report 2013-2014* at 43, online (pdf): <www.ocsec-bccst.gc.ca/a37/ann-rpt-2013-2014_e.pdf> [perma.cc/4NH9-L7G8].

planning process for it. The Jordanian intelligence includes metadata of a call between a Hezbollah affiliate and Bob. Bob and Yves, in the meantime, did discuss a gathering at their café meeting, and one later took place in suburban Ottawa.

The dots connect in this hypothetical in a manner that simplifies life and this article includes only the "signal" and none of the "noise" that would make piecing together puzzles difficult. But in this scenario, CSIS should now be preoccupied with sharing some information with the RCMP. In principle, the Jordanian-origin metadata and the CSE intercept could be "evidence" in a criminal proceeding. However, to use it would raise I2E concerns about secondary materiality. For example, if the CSE intercept were used to help prove a terror plot, facts concerning the circumstances of this intercept and how it was conducted might become material. What sort of technology was used, for example, to trace the call to CP A, and how can one be sure that CP A was the person on the call? The CSE will not willingly part with the sensitive information needed to satisfy this line of inquiry.

But still, we have enough that hints at a possible terrorist plot or other criminality, and in the interests of both public safety and "de-confliction" between the CSIS right-hand and RCMP left-hand, the RCMP should be told something. In practice, in this case, they would likely be given a hint, in the form of a so-called "disclosure letter." This will be just enough information to allow the RCMP to start its own investigation,[85] but not so much to tie CSIS into a joint investigation that might sweep its full intelligence investigation directly into the *Stinchcombe* regime.

That means that enough is shared to allow RCMP and CSIS to realize that they had been working on different aspects of the same matter: they had both surveilled the gathering at the suburban house in Ottawa. And both the RCMP and CSIS can link Trent (the suspected passport forger), Bob and Yves (the suspected Hezbollah sleepers). And so, the RCMP and CSIS now begin a deconfliction process to manage what becomes two, parallel investigations into the same suspected plot: the police criminal investigation (now called Operation PARTY) and the continuing CSIS security intelligence investigation. In doing so, they follow the inter-agency framework designed to supervise – without fusing – this segregated

---

[85] A disclosure letter "contains information designed to provide an investigative lead that the RCMP may use to initiate its own investigation. The information in the disclosure letter is not to be used as evidence by the RCMP without prior consultation with CSIS." One Vision 2.0, *supra* note 59.

investigative system: One Vision (now in its second version as "One Vision 2.0").[86]

Fortified with all this new information, CSIS is closer to the "reasonable grounds to believe" standard required for a CSIS Act wiretap warrant. Of course, to obtain this warrant, it would need to use the Jordanian and CSE information, a prospect that neither source would embrace with relish. But we shall assume that caveats are relaxed, carefully crafted affidavits are prepared, and the Federal Court authorizes a CSIS wiretap warrant on both Yves and Bob.

F. The Wiretapped Call

Very soon after, CSIS intercepts a call between Bob, Trent and Yves. In it, the three men talk about "making new false passports for the brothers in Syria" and discussing "joining Hezbollah fighters in Syria." This is direct evidence of crimes. It would be admissible as relevant evidence of a material fact in prosecutions for terrorism travel[87] and passport fraud.[88] It is information that the RCMP might reasonably wish to have as a form of actionable-intelligence in a police investigation.

Does CSIS share this intelligence, this time in what is known as an advisory letter containing these investigative fruits? The answer should be "yes." But CSIS may worry that the contents of its wiretap intercept, used to further an RCMP investigation, may then attract scrutiny of its own Federal Court warrant and the basis for it. And since that CSIS warrant is built on foreign origin intelligence and signals intelligence, it would not wish too close an inquiry in open-court into the evidence buttressing the Federal Court wiretap authorization. And things are not that urgent yet. There is no intelligence suggesting that Yves and Bob are an imminent risk to public safety, although they seem to have malevolent designs.

Still, without the supplemental CSIS information, the RCMP is not likely to have enough evidence so far to obtain its own search and wiretap warrants. Its investigation is stuck, in consequence, with other, less invasive investigative techniques. That would mean that the agency with the most forceful capacity to disrupt a threat – the police – is partially in the dark about the development of that plot.

---

86 *Ibid.*

87 *Criminal Code*, *supra* note 45, s 83.181.

88 *Ibid*, s 57.

It is not certain to me that CSIS would share the content of its intercept with the police – under the One Vision 2.0 framework, that choice rests with it.[89] There is no legal obligation to disclose this information,[90] and CSIS may decide that the public safety imperative is not grave enough to risk *Stinchcombe* disclosure of shared information. But, nevertheless, I shall assume CSIS provides police with an advisory letter that contains the substance of the intercept: namely, that Trent, Bob and Yves are plotting joining Hezbollah in Syria and providing false passports to its members. This, along with information from the RCMP's original investigation of Trent, is packaged into a separate police affidavit that then is used to obtain a police wiretap authorization.

G. Reaching for Tools

CSIS does have other legal tools. Under Canadian law, passport revocations and listing on Passenger Protect (the no-fly list) can be done administratively, using classified evidence that can then be preserved from disclosure to the interested party or the public in any subsequent appeal. Likewise, Yves is a foreign national, and immigration removal proceedings (under the "security certificate" regime or otherwise) can be conducted behind closed doors, using classified information. Here, intelligence can be used as an evidentiary-intelligence sword, because it is shielded from open disclosure.[91]

This is not to say that CSIS information will go untested in the event these matters end up before an adjudicator. That adjudicator will require evidence in any appeal or removal proceeding. The rules of evidence are not as strict here as they would be in a criminal proceeding. For instance, hearsay may be used in immigration security certificate proceedings, if the Federal Court judge regards it as "reliable and appropriate, even if it is inadmissible in a court of law, and may base a decision on that evidence."[92]

---

89 One Vision 2.0, *supra* note 59 at 5.

90 CSIS does have the discretion to disclose under CSIS Act, *supra* note 6, s 19(2).

91 See, respectively, *Prevention of Terrorist Travel Act*, SC 2015, c 36, s 42 at ss 5-6; *Secure Air Travel Act*, SC 2015, c 20, s 11 at s 16; *Immigration and Refugee Protection Act*, SC 2001, c 27, Division 9 [IRPA].

92 IRPA, *supra* note 91, s 83(1)(h). *Almrei (Re)*, 2009 FC 3 at para 53 (This section "permits the reception of hearsay evidence such as that which may be provided by a confidential informant or a foreign intelligence service."). See also *Harkat*, 2014 SCC 37 at para 75.

Still, hearsay may diminish the weight given to this intelligence, and raise questions about procedural fairness.[93] And it is likely specially-cleared independent lawyers (known as "special advocates" or *amici curiae*) will be tasked by the adjudicator to probe aspects of the government's case. In the immigration security certificate context, CSIS has used information acquired through confidential sources, communicated through the proxy of an intelligence officer. The government has no obligation to produce the source. However, the Federal Court has affirmed it (and special advocates) must nevertheless be able "to effectively test the credibility and reliability of that information…To conform to the law, CSIS and the Ministers must give the Court all of the information necessary to test the credibility of the source and not just the information that a witness, trained as an intelligence officer, considers operationally necessary."[94]

But even if CSIS is comfortable with this degree of limited disclosure (and it may not be), these security certificate, no-fly or passport revocation processes would alert the targets of investigation to the existence of that investigation, something that would be prejudicial to further unraveling this conspiracy. In our hypothetical, CSIS decides it is better to keep the investigation covert, to determine its full extent.

H. The Plane Ticket

CSIS investigators determine Trent has now booked a plane ticket to Turkey, a common gateway to Syria. CSIS could somehow use its "threat reduction" powers to delay and possibly stop Trent's travels – although it is difficult to see how it could do so indefinitely, without exposing the investigation. It could place Trent on the no-fly list and revoke his Canadian

---

93 See e.g. *Harkat*, 2014 SCC 37 at paras 76, 235 (suggesting judges are able under the security certificate process to "exclude not only evidence that he or she finds, after a searching review, to be unreliable, but also evidence whose probative value is outweighed by its prejudicial effect against the named person."); *Mahjoub (Re)*, 2013 FC 1097 at para 130ff. (concluding that hearsay evidence may be admissible in security certificates, but must be tested for reliability and appropriateness); *Zundel (Re)*, 2004 CF 1308 at para 25 (indicating in a security certificate context that "hearsay evidence is given less weight").

94 *Harkat (Re)*, 2009 FC 1050 at para 48. See also *Canada (Citizenship and Immigration) v Harkat*, 2014 SCC 37 at para 88 ("The Minister has no obligation to produce CSIS human sources as witnesses, although the failure to do so may weaken the probative value of his evidence") and para 90 (noting that "the designated judge's weighing of the relevant [source] evidence took into account the fact that it was hearsay").

passport, but again that would expose its covert investigation. Alternatively, it could notify the Turks, but at the risk that the Turks would then detain an arriving Trent and mistreat him. Where this risk is substantial enough and cannot be mitigated, CSIS is barred by ministerial direction from sharing this intelligence with its Turkish partners.

In these circumstances, especially since there is no reason to believe that Trent-the-suspected-passport-forger poses an imminent public safety risk, the best thing may be to let Trent conduct his trip, subject to whatever continuing surveillance CSIS (likely with CSE's assistance)[95] can mount.

The police, who independently learn of Trent's plans from their new wiretap on him, come to a similar conclusion: if they were to arrest Trent, they would have little evidence of why he was travelling to Syria that did not come from the original CSIS intercept. Moreover, Bob and Yves would be alerted, and the prospect of obtaining more evidence on those plotters would evaporate.

I. The Confidential Source

Meanwhile, a fourth individual, Alice, contacts local police in Ottawa, expressing worry that "a couple of her friends are going down the wrong path." She provides enough details that the police believe that this may be a terrorism matter, and they pass Alice on to the RCMP (likely operating through Ottawa's Integrated National Security Enforcement Team). It turns out that Alice is Bob's roommate, and she is worried that Bob wants to build a bomb.

The RCMP quickly tie this new information into Operation PARTY, and they pass on the new information to CSIS. The police might be tempted to now arrest Bob, but the information that could be used as evidence tying Bob and Yves and Trent to a bombing plot orchestrated by Hezbollah is still weak, especially if the intelligence sources cannot be used.

Both the RCMP and CSIS think, therefore, it would be wise to manage Alice as a confidential informant. The police would like to do so, as part of building a criminal case. But if CSIS is not willing or able to share the full-fruits of its own investigation with the RCMP, the police may find it difficult to run Alice as an informant without risk to Alice, or to the two parallel investigations. This is especially true if CSIS hopes to cultivate Alice as a long-term source, possibly implicated in other investigations. I am not sure

---

95 CSE may provide technical assistance to CSIS under its so-called "Mandate C". *National Defence Act*, *supra* note 83, s 274.64(1)(c).

what would happen in this case, but will assume that Alice becomes a CSIS confidential informant.

J. The Emergency

Days later, Alice contacts her CSIS handler and reports her belief that Bob and Yves are planning to drive a rented truck into a music festival in Ottawa on Thursday, in protest of the Canadian Armed Forces presence in Syria.

There is now an imminent public safety risk, and the plot has clearly moved to a conspiracy cognizable as terrorism criminal offences. But proving this would depend on Alice's cooperation, and she tells CSIS she will not testify in court. Meanwhile, Bob and Yves have gone "dark" – there is no electronic communication, or that communication is fully encrypted (a commonplace reality now).

The authorities confront a dilemma. CSIS issues an advisory letter to the RCMP. At the very least, steps need to be taken to harden the festival site, and that requires police involvement. But the police still do not have the evidence for a conventional arrest for this latest plot, let alone a prosecution, if Alice will not cooperate. It seems unlikely they would even have enough evidence to make out a case for a preventive detention (technically, a recognizance with conditions).[96] The fact that Bob and Yves have rented a truck is evidence of nothing, since it does not prove what they intend to do. Indeed, the truck plot is a departure from what appeared, earlier, to be a bomb plot. Proof of a truck attack would depend entirely on Alice's testimony, and she is not cooperating.

If CSIS supplied the fruits of its full investigation, the police could possibly obtain a peace bond,[97] imposing some constraints on Bob and Yves. If the police could rely on the fruits of the CSIS wiretaps and their own information on Trent and his travels, they might be able to charge for conspiracy to commit passport fraud, a proxy form of preventive "charging down" to stave-off a more serious threat. But both approaches would culminate an open-court process, and CSIS and the police again worry about the evidentiary-intelligence issues. The two services debate the matter, but since there is no one above the two agencies overseeing the investigation and deciding whether to prioritize information or intelligence or evidential

---

96 *Criminal Code*, *supra* note 45, s 83.3.

97 *Ibid*, s 810.011.

purposes, CSIS reluctance to relax its caveats on its information carries the day.

CSIS then makes the decision to deploy its threat reduction powers, and covertly disable the rental truck acquired by Bob, in a manner ensuring it does not start. Since sabotage would break Canadian law, it obtains a warrant from the Federal Court, something it can do using intelligence in a closed-door session, with Alice's identity minimized.[98]

And so, when Bob and Yves try to start the truck on Thursday morning, its engine will not turn over. Because CSIS has been careful, the plotters attribute this fact to a faulty truck and do not suspect that they have been discovered. And so, the parallel investigations remain on track.

But the plotters are frustrated. CSIS and the RCMP continue to follow the men, following their deconfliction protocols to avoid tripping over each other. The next morning, as he does every day, Yves takes the city bus to his workplace in the food-court at Ottawa's Rideau Centre, right next to the Department of National Defence headquarters. He approaches his workplace, as he does every day, passing several uniformed military personnel enjoying their early morning coffees. Suddenly, he takes a large knife from his backpack and repeatedly stabs the nearest armed forces member, gravely wounding him. The CSIS surveillance team – unarmed – can do nothing. But police arrive on the scene and Yves is killed as he continues to resist arrest and threaten members of the public.

In the weeks after, Bob leaves Ottawa and, along with Alice (still a CSIS informant) moves to Toronto. Under continued expensive surveillance by CSIS and the police, he keeps a low profile. That is, until he commences the bomb plot with which this paper began. And the cycle begins again.

K. The Intelligence "Failure"

In the media and in the National Security and Intelligence Committee of Parliamentarians inquiry that follow, the Rideau Centre attack is characterized as an "intelligence failure." CSIS and the RCMP are roundly criticized, and their brass hauled before parliamentary committees. Parliamentarians respond by enacting new criminal law, making terrorism crimes punishable thrice-over, and giving CSIS new powers to detain people for security intelligence purposes, raising inevitable concerns about secretive detentions by an intelligence agency. Constitutional challenges follow, with

---

98 CSIS Act, *supra* note 6, ss 12.1, 21.1.

the typical negative collateral reputational consequences for the security services.

Like usual, all this political *sturm und drang* misses the point. There is no deficit of agency powers. There is no failure in the collection of information, and thus no intelligence failure. No one acted with malice. No one was incompetent. Every decision made reflected a reasonable response, at the time, to a dilemma.

The failure stemmed, instead, from the very existence of that dilemma: intelligence-to-evidence. Fear over the evidentiary-intelligence issue restrained actionable-intelligence sharing, and open court responses built on it. In the result, a victim is gravely wounded, the remaining bad guys are still not in jail, and politicians misdiagnose the problem as a nail, for which the solution must be a bigger hammer.

VI. Reform

Would there be a better way to resolve the Bob the Bomb-Builder hypothetical? The scenario is obviously a simplified, artificial one. It could be that the degree of information-sharing and deconfliction between RCMP and CSIS would be much greater than I have allowed – those who commented on drafts of this paper were divided on this issue. Moreover, the fact that the plotters went "dark" at a critical point suggests another important issue not addressed by this paper: questions of encryption, lawful access and investigative techniques.

Still, I am persuaded that this hypothetical is realistic enough to underscore the sorts of dilemmas CSIS and RCMP confront in terrorism investigations. And from an I2E perspective, the obvious pivot point in this hypothetical was the decision not to charge Bob, Yves and Trent with conspiracy to forge passports, as a means of incarcerating them once the public safety risk became acute. A prosecution would have required use of the CSIS intercept information, as evidence of guilt. But an arrest and charging of the three plotters would have placed them behind bars, and forcefully disrupted a dangerous situation.

Perhaps my hypothetical is a disservice, and that this is exactly what would have happened. It would be easy, however, to change the facts to make the I2E dilemma even more acute. And so, the topic that deserve attention is this one: what changes in I2E would have made this interruption in the life-cycle of a plot like this the more likely outcome? One

school of thought, expressed most vigorously by the Air India bombing commission, is that I2E is best solved at the back end, with a reformed *Canada Evidence Act* s. 38 process involving a single trial judge. This would eliminate the arduous bifurcation between a trial judge (overseeing the criminal trial) and the Federal Court judge (deciding whether to extend an evidentiary-intelligence shield).

There are good reasons – not least judicial efficacy and swifter trial processes – for reforming Canada's bifurcated s. 38 system. I support efforts to streamline the s. 38 process.[99] But this is not the rocky shore on which I2E reform founders. Fixing s. 38 is unlikely, alone, to solve I2E. The I2E dilemmas in the Bob the Bomb-Builder hypothetical are not driven by "which court will decide whether CSIS's sensitive means and methods will be sheltered from *Stinchcombe*." They stem, for CSIS, from the uncertainty of whether they will be sheltered.[100] Averting to figure 1 above, the problem with s. 38 is uncertainty as to whether shared information will fall into zone AB2 or AB3. Uncertainty on this issue also affects the police. Should they build the case on the foundation of sheltered CSIS intelligence, the failure to disclose that foundation will culminate in a finding by a court that the trial is not fair. The parallel investigation strategy, linked only by disclosure letters and, less often, advisory letters, is fueled by this uncertainty.

In sum, s. 38's ambiguous balancing test does create uncertainty – although it is important not to exaggerate. After all, the Attorney General can cure aberrant disclosure orders with an Attorney General's certificate. But more important sources of uncertainty come in several other guises: What exactly does *Stinchcombe* mean by "clearly irrelevant"? Or put another way, what is the boundary in figure 1 between zone B and zone AB2. Risk adverse prosecutors are likely to conflate "relevance" with "everything" in an information-holding, but as argued above "relevance" is not the same as "everything." Relevance is determined by the trial, not the original investigation.

Another uncertainty is: what is the precise point at which a CSIS and police investigation are so intertwined as to attract the *Stinchcombe* standard for both police and CSIS investigations? Put another way, how big is zone

---

99 See Forcese & Roach, *supra* note 7 at chapter 9.

100 See the discussion on this point in Leah West, "The Problem of 'Relevance': Intelligence to Evidence lessons from UK Terrorism Prosecutions" (2018) 41:4 Man LJ 57.

C? Without guidance, risk adverse security services are likely to use a 10-foot pole to hold each other apart, even if a metre stick would suffice.

Step 1 in solving the I2E dilemma is, therefore, to create certainty, in a manner that increases the size of actionable-intelligence in zones AB1 and AB2 – that is, information shared by CSIS that can be used by police. Not all I2E dilemmas can be solved by mere certainty, but certainty would ensure that the ones that do arise are real, and not assumed or feared. Certainty would allow risk to be managed. In the balance of this article, I propose steps moving us further down that path. And I repeat my admonishment at the outset of this paper: solving I2E is a game of Moneyball, in which regular base hits are better than occasional home runs.

A. Forward Planning and Managing the Relevance Tear-line

I2E solutions should grow the size of zone AB2, and minimize Zone C. CSIS anti-terrorism investigations should be managed so as not to jeopardize the prospect of prosecution. In practice, that means they should be organized as if disclosure was a possibility (because it always is, even now). And that requires planning. If – because of early, close collaboration with specialized, seconded prosecutors – a CSIS anti-terror investigation is undertaken with an understanding of the likely breadth of the relevance window, CSIS will have a better chance of knowing what information will be within the disclosure "tear-line" of zone B, and what information is outside it. And it can manage its investigation accordingly.

For instance, the information likely to form zone AB when shared should be collected to "evidential standards." By this, I simply mean it is managed in a manner most able to survive court scrutiny. For example, do not rely on analytical summaries of destroyed intercept recordings. Ensure continuity and integrity in the information, in the sense that it can be sourced, explained and addressed in testimony. Physical items seized as part of the investigation (not a likely prospect for CSIS anyway) should be properly logged, and chain of custody preserved. Surveillance teams should be trained on how to present evidence, prepare logs and make witness statements. Like their UK MI5 counterparts,[101] CSIS officers should be prepared to testify in court, with protections designed to guard their identities.

---

[101] UK Security Service, "Evidence and Disclosure" (last visited 13 May 19) online: <www.mi5.gov.uk/evidence-and-disclosure> [perma.cc/9LHY-9SEV].

Collection to "evidential standards" should also mean that the Crown jewels – information CSIS cannot disclose without prejudice to its operations – should not be irremediably muddled with information within the relevance tear-line. For instance, if a video is made of an informant interacting with a target, it should be produced in a manner that does not compromise that informant's identity protection automatically. Film the encounter with the informant's back to the camera.

Institutionally, the only way to accomplish these objectives is to incorporate evidential thinking at the genesis of any anti-terrorism investigation. The obvious reform step here is to involve specialist prosecutors seconded to CSIS (but not themselves charged with prosecuting any resulting crimes) early in any CSIS terrorism investigation. Indeed, they need not even be employees of the Public Prosecution Service of Canada. The key prerequisite is: prosecutorial, criminal law and investigative expertise, certainly not institutional affiliation. These legal experts would not themselves be the "Crown" in any subsequent prosecution, and therefore would not have their own disclosure obligations. But seconded as a form of operational assistance, they may be able to assist in managing the relevance tear-line,[102] by envisaging creative solutions such as "Al Capone" charging.

This concept of "Al Capone" or "preventive" charging requires some explanation. Whether under the *Stinchcombe* or *O'Connor* standard, the gravamen of disclosure is "relevance." "Relevance," at common law or under the *Charter*, is tied to materiality. And materiality is tied to the issues before a court in a legal proceeding. Where the Crown controls those issues – by, for example, choosing to lay one charge rather than others – it also affects the aperture of the relevance concept. In my hypothetical, the Crown could have moved against Bob, Yves and Trent for conspiracy to engage in passport fraud. "Conspiracy" depends on an intention to agree, the completion of an agreement, and a common design, all linked to the commission of an indictable offence.[103] Passport fraud requires, simply, forging a passport.[104] The unambiguous statements made by the plotters on the CSIS wiretap – coupled with whatever the police had on Trent that had sparked their initial investigation – could have been enough to sustain the

---

102 For a discussion of the role of specialized Crown Prosecution Service lawyers managing complex terrorism cases in the United Kingdom, see West, *supra* note 100.

103 *United States v Dynar*, [1997] 2 SCR 462 at para 86, [1997] SCJ No 64.

104 *Criminal Code*, *supra* note 45, s 57(1)(a).

conspiracy charges. The evidence relevant to this charge is everything that, as a matter of logic, makes it more probable (or not) that the plotters conspired to forge a passport. Obviously, the core evidence would be the CSIS intercept. But even if *Stinchcombe* applied, it is hard to see how any of the rest of the CSIS file about Hezbollah and Jordan and CSE is relevant to a fact material to this case, because of the charge laid. This would be true even for the police, had this intelligence been shared with them. Put another way, much of the CSIS information from the broader investigation would be in zone A, or if shared, zone AB1 of figure 1.

But should the Crown also charge the men with a terrorism offence, it would likely need to prove the predicate aspects of "terrorist activity" found in *Criminal Code* s.83.01, including that the men committed their offence "in whole or in part for a political, religious or ideological purpose, objective or cause, and ...in whole or in part 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, whether the public or the person, government or organization is inside or outside Canada." The scope of information that is relevant to these new matters expands immensely.

There would be a lot more in the CSIS investigation file relevant to the terrorism offence charge – and especially the men's intent and motive – than is relevant to the conspiracy to forge a passport charge. Put another way, more information would be in zone AB2 (disclosable under *Stinchcombe*) or zone C (disclosable under *O'Connor*). And so here, if it had disclosure obligations, CSIS would need to worry about protecting its intelligence secrets, using *Canada Evidence Act* s. 38. It could probably do so, but the Crown could not then use all this intelligence on motive and purpose. And the case might be lost.

Managing the relevance tear-line may require, therefore, applying the Al-Capone strategy: mobster Capone was never charged with mobsterism, but rather tax fraud. In the same spirit, bad guys may be charged with the offences with the narrowest aperture of relevance.[105] This requires no legal change and raises no legal doubts. It depends instead on a careful appreciation of existing legal concepts. And it requires premeditation and planning.

---

[105] This is precisely the approach applied in the United Kingdom. See discussion in West, *supra* note 100.

B. Managing Witnesses

Part of this planning should include consideration of how to protect the identity of witnesses and intelligence officers, even while using their testimony. There is no prospect of a fully-closed trial on the merits in criminal matters (although there is, I believe, the prospect of closing collateral aspects of a criminal case, as discussed below in relation to *Garafoli*). The accused has a right to confront their accuser, and I cannot imagine any system, short of a derogation from the *Charter*, that would permit closed proceedings on the merits in criminal trials.

But that does not mean that a trial must be fully open to the public. Put another way, it is possible to have aspects of a trial, *in camera*. This would exclude the public (and media) but not the accused and their counsel. In colloquial language, we sometimes call this a "publication ban" and it is captured by the so-called "Dagenais/Mentuck" test. Courts are presumptively open in Canada. Under the Dagenais/Mentuck test, "public access will be barred only when the appropriate court, in the exercise of its discretion, concludes that disclosure would subvert the ends of justice or unduly impair its proper administration."[106] The prospect of *in camera* proceedings (and testimony behind a screen) on national security grounds is now codified in s. 486 of the *Criminal Code*.[107]

Whether careful use of s.486 would relieve anxiety about source protection or other concerns CSIS might have about have about participation in criminal proceedings is unclear to me. Section 486 would not change the pre-trial disclosure obligations. And it would not protect identities from the accused or his or her lawyer. The witness would confront real risks if the accused is, in fact, a threat actor. Witness protection may not be enough to appease many witnesses. But testimony behind screens would at least limit widespread diffusion through the media.

C. Understanding the Third-Party Threshold

Managing the tear-line means adjusting the size of zone B, and the aperture of *Stinchcombe*. Collecting to evidential standards minimizes the

---

106 *Toronto Star Newspapers Ltd v Ontario*, 2005 SCC 41 at para 4.

107 See also Canadian Broadcasting Corp v New Brunswick (Attorney General) (Re R v Carson), [1996] 3 SCR 480, [1996] SCJ No 38 (upholding the provision under s 1 of the *Charter*).

prejudicial impact of being subject to *Stinchcombe*. Managing witnesses reduces, potentially, the scope of source identity diffusion.

CSIS may, however, still wish to preserve third-party, *O'Connor* status (at least for portions of its investigation and information). The *O'Connor* standard does not change the ultimate standard of disclosure to something other than "relevance."[108] It does, however, make it harder for the defence to obtain CSIS disclosure, avoiding defence fishing-expeditions. And CSIS may feel this extra comfort is required, especially since it may not be possible to manage the tear-line perfectly. There will be cases where there is no viable Al-Capone strategy. Imagine, for instance, that police continue to investigate Bob. They intercept a telephone call between Bob where he espouses a violent ideology and lays out the details of a bomb plot. They lay terrorism offence charges. While the prosecutor's case may be built entirely on police evidence, the relevance "tear-line" now extends far into CSIS's holdings, since there is much in CSIS's possession that might relate to Bob's terrorist motive – that is, much information in zone C. If CSIS and police were both subject to first-party *Stinchcombe* disclosure obligations, all that zone C information would be disclosable, subject to a successful s.38 proceeding. CSIS might, therefore, welcome the prospect of *O'Connor* third party status.

Even this may be a thin reed in practice – *O'Connor* increases the burden on the defence to show likely relevance. But once established, third-party status does not then render relevant CSIS information non-disclosable, unless other (privacy) issues balance against the fair trial interest. I doubt these other issues will often prevail. For one thing, "absent an overriding statutory regime governing the production of the record in question, a third-party privacy interest is unlikely to defeat an application for production."[109]

It is true that the Supreme Court has found constitutional a legislated rule that extends third-party status to, and limits disclosure of, certain "private record" information even within the Crown's possession.[110] In doing so, however, it had close regard to the robust privacy interests a person might have in things like medical or psychiatric records, especially in circumstances where the defence wishes to use the records to undermine the credibility of sexual assault victims. The policy justification for a similar approach to CSIS documents – preserving investigative targets, means,

---

108 On this point, see the discussion in *McNeil*, *supra* note 33 at paras 39, 47.

109 *Ibid* at para 41.

110 *R v Mills*, [1999] 3 SCR 668, [1999] SCJ No 68.

methods and sources – is not as persuasive. The state does have a strong interest in keeping these records confidential – but there will be fewer individual privacy interests in play.[111] While courts have readily recognized the importance of keeping intelligence secret,[112] the means for doing so is already provided by s. 38 of the *Canada Evidence Act* or other source identity protection rules. I doubt the need substantively for repeating and duplicating these protections in a legislated, *O'Connor* second prong.[113]

In these circumstances, third-party status may be useful. However, because it imposes more of a procedural than substantive means of protecting CSIS secrets, it is not the hill to die on. It is probably not even a slight-rise to die on. Still, I appreciate it might still be proper and appropriate at times, so long as it is structured to minimizes the negative consequences of third-party status, especially to public safety. The police and CSIS investigations should be dovetailed as closely as possible, while still maintaining third-party distance.

It is, however, painfully unclear where the line between third-party and first-party status lies. The parallel investigation structure – where CSIS and RCMP deconflict, but where CSIS provides carefully-curated information through disclosure and advisory letters – lies short of the line.[114] But it may also be more conservative than it needs to be. Based on past caselaw, the operational ingredients of this sort of parallel investigation include the following:

Table 2: Facts Cited in Past Cases on CSIS Third-Party Status[115]

	CSIS Investigation	Police Investigation
Structure	Investigative relationship between CSIS and police governed by a memorandum of	

111 The exception would be source identity, but that is already protected by source identity protections in the CSIS Act, *supra* note 6, s 18.1

112 See e.g. *Charkaoui v Canada (Citizenship and Immigration)*, 2007 SCC 9 at para 68 [*Charkaoui*].

113 If this were a question of "either/or" I would prefer to see the balancing done by a trial court as part of a legislated *O'Connor* than by the Federal Court in a collateral *Canada Evidence Act* proceeding. If there were a question of "both," the only likely outcome is: longer, more complex trials.

114 See the discussion of this parallel investigation system, in the context of *O'Connor* disclosure, in *R v Ahmad*, *supra* note 1.

115 Drawn from *ibid*.

	understanding, governing information-sharing and the maintenance of separate investigations.	
Initiation	Initiated for security intelligence purposes.	Initiated for criminal investigation purposes.
Timing	CSIS investigation first in time.	Police investigation prodded by initial CSIS tips, in response to public safety concerns.
Scope	Broad international and national investigation.	Narrower investigation, focused on specific individuals in Canada.
Control	CSIS runs its investigation, and is free to disregard police views.	Police run their investigation, and are free to disregard CSIS views.
Cooperation	Interaction limited, to maintain firewall, with CSIS insulated from the street-level police investigators. CSIS embedding with police about feeding police information to CSIS, not the vice versa. At the management level, cooperation about resolving possible confliction of investigations and to keep a wary eye on public safety.	
Information-sharing	Carefully controlled substantive CSIS information sharing with police through disclosure and advisory letters, with information held back even when it could have assisted the police. Where information shared by CSIS on a less structured basis, done for a clear public safety basis. Logistical, deconfliction meetings restricted to ensuring operational awareness between the agencies. Freer flow of information from the police to CSIS, allowing CSIS to remain on top of an investigation and hold-back somewhat in terms	

	of pursuing their investigation to avoid confliction.
Sources	Effort to keep management of sources discrete, between agencies. Where CSIS source handed over to police, effort to create a "clean break." After a handover, CSIS no longer gives instructions to the source.

But this is simply a laundry list of facts that supported the existence of third-party status. The unanswered question is whether each of these elements must be present legally to maintain CSIS third-party status. No court has so asserted. Indeed, the generic criteria for the line between first- and third-party status, to the extent they have been summarized,[116] are less rigid:

- CSIS initiated its investigation as a real security intelligence investigation, not to prosecute an accused;
- CSIS and police did not have full access to each other's files; and,
- CSIS did not take an active role in or direct the police investigation.

Precision as to the line between first and third-party status would be useful. Nothing stops Parliament from legislating statutory third-party status for intelligence services[117] – as noted, legislated third party status exists in other contexts, and indeed reaches information in the hands of the Crown. Put another way, information is given third party status, because of its origin and nature.[118] And, to repeat, there is no reason to assume that the legislated line must produce the same degree of distance maintained in practice between CSIS and police, out of an excess of caution. Indeed, it may be possible to defend a line that encapsulates only the three expectations above. At minimum, therefore, clear statutory guidance should extend the *O'Connor* test to CSIS where: CSIS's investigation is a *bona fide* security intelligence investigation; police, at least, do not have full, unmediated

116 *Ibid* at para 12.

117 For a discussion on legislating third-party status for CSIS, see West, *supra* note 100.

118 See *Criminal Code*, *supra* note 45, ss 278.1, 278.2(2)ff, relating to third-party records containing the personal information of a complainant or witness. See also *McNeil*, *supra* note 33 at para 21.

access to CSIS files; and, CSIS does not take an active role in the police investigation.

But any legislated third-party status should not maintain rigid barriers on information-sharing as one of its ingredients. Parliament might reasonably maintain the CSIS is still engaged in a *bona fide* security intelligence investigation, whose purpose is not prosecution, even with close information-sharing. The key issue should remain whether CSIS's information satisfies the suppositions undergirding *Stinchcombe*: the agency does not have the information for criminal law purposes, and therefore its information holdings are not likely relevant and do not comprise the case against the accused. Unless the defence can show that the CSIS investigation is a "stalking horse" for a criminal proceeding, the justifications for *Stinchcombe* would be absent.

There is no compelling policy reason to fear this stalking horse. A CSIS investigation is not an activity undertaken by an agency with fuller, regulatory access to private information than the police. CSIS investigations are subject to police-like *Charter* obligations,[119] where invasive. CSIS warrants are issued on different standards than police warrants because CSIS investigates diffuse threats and not discrete crimes, but it is wrong to suggest they are laxer or less privacy-protective.[120] Movement of information from a CSIS investigation to a police investigation does not, therefore, raise policy concerns about end-runs around constitutional privacy protections.

In sum, in the Bob the Bomb-Builder hypothetical, it should have been possible for CSIS to share its intelligence earlier and in more detail without losing its third-party status.

---

119 *X (Re)*, 2017 FC 1047 at para 168.

120 For a discussion of the different scope of CSIS vs police warrants, see *Huang* FCA, *supra* note 62 at para 33. In 1988, the Federal Court of Appeal concluded that the CSIS warrant system fulfilled *Charter* s 8 requirements in *Atwal v Canada*, [1988] 1 FC 107 (FCA), [1987] FCJ No 714. Kent Roach has discussed whether the fruits of CSIS warrants introduced in criminal proceedings might be deficient because they did not meet crime-based reasonable grounds. He has suggested that even if they violated s 8 standards in these circumstances, they might be upheld under s 1, so long as the CSIS warrant was not being used as a short-cut around a Criminal Code warrant. Roach, *supra* note 4 at 90ff. Since that time, it is worth noting that some police authorizations for things like transmission data (metadata) recorder may now be obtained on reasonable grounds to suspect grounds. See Criminal Code, *supra* note 45, s 492.2. CSIS, meanwhile, would need to meet a reasonable grounds to believe standard for the same information. There is reason to believe, therefore, that CSIS warrants are more demanding on the state than at least some Criminal Code authorizations.

D. Managing *Garafoli*

Some of the shared CSIS information would be the product of a CSIS wiretap. If the police had arrested Bob, Yves and Trent on conspiracy to forge passports, the evidence for that charge would stem from the CSIS intercept. That means that the aperture of relevance could extend to the warrant process leading to the intercepted information. And in the hypothetical, the CSIS Act warrant was supported by signals and foreign-origin intelligence.

In a *Garafoli* challenge to the warrant, where the CSIS information was used to bring passport fraud conspiracy charges, the defendant would almost certainly be entitled to the warrant and supporting affidavit. Affidavits should be prepared in anticipation of this disclosure, and drafted in a manner that squares the necessity of persuading the issuing judge with the prospect that the affidavit may become public.

Source intelligence not before the judge in support of the warrant application is not generally disclosable. Recall that "relevance" in this context is tied to challenging the warrant. The defence would need to persuade a court that this extraneous material would tend to discredit the warrant authorization. This narrow concept of relevance does not authorize a fishing expedition through documents not before the affiant whose affidavit supported the warrant application. There is also the possibility the CSIS affiant may be cross-examined, but only with leave of the court persuaded it could discredit the CSIS Act authorization and confined to the question of whether the affiant knew or ought to have known about errors or omissions in the warrant application. Out of caution, CSIS warrant teams should be firewalled from information that is, in fact, extraneous to the merits of the warrant application, and trained also in how to best present in court.

Nevertheless, despite these safeguards, there may be much in a CSIS warrant application that CSIS will wish to protect, especially where the warrant is built on foreign and signals intelligence. It will be tempted to use s. 38 to protect this information, but at risk that this non-disclosure will lead a trial judge to conclude that the warrant was impaired or a fair trial is compromised.

The question is, therefore, whether there are other means of narrowing the risk of full disclosure. Specifically, must the *Garofoli* challenge be conducted in open court, with the full participation of the accused and their counsel? This is a novel question, and the mere prospect of a closed process

would ignite condemnation from the defence bar. But given the Supreme Court's jurisprudence on closed-door national security proceedings, I believe such a proceeding would be constitutional.[121] In a *Garofoli* proceeding, neither the guilt nor innocence of the accused is at issue.[122] The focus is entirely on what information was before the warrant-issuing judge, and whether it meet the legal thresholds applicable to that earlier *ex parte* and *in camera* warrant process. Here, neither the accused nor his or her lawyer marshal new facts to second-guess, retrospectively, the warrant. The only value-added they provide is adversarialism. That is, they are motivated to test the legitimacy of the warrant. Yet, there are other means of accomplishing this testing: security-cleared special advocates.

It is near inconceivable to me that a court would find unconstitutional the substitution of a special advocate for defence counsel in a closed *Garofoli* challenge implicating national security information. Such substitutions have been permitted in circumstances much more impairing of due process preoccupations. For example, accused and their counsel are excluded from *Canada Evidence Act* s. 38 proceedings – and here there is no obligation even for a special advocate, although courts have often tasked near-equivalent *amicus curiae* with testing the government's position. A closed s. 38 system is not a trivial exclusion of defence counsel – after all, it is the defence that will be in the best position to gauge the impact non-disclosure would have on their case.[123] And yet, the s. 38 process is constitutional.[124]

Even more significant is the Supreme Court's jurisprudence in the immigration security certificate context. Here, named parties are denied access to classified information used against them, on the *merits* (and not simply on a matter collateral to the merits). This system violates *Charter* s. 7, but is saved under s. 1 where special advocates are present in the closed proceedings to challenge the government case.[125] Notably, the Supreme Court has upheld this arrangement,[126] even while acknowledging that the possible consequences of a security certificate – especially, the prospect of

---

121 On this point, see also Roach, *supra* note 4 at 113.

122 See *R v Pires; R v Lising*, *supra* note 34 at para 30 ("the *Garofoli* review hearing is not intended to test the merits of any of the Crown's allegations in respect of the offence.")

123 On this point, see *Huang*, *supra* note 27 at para 48.

124 *Ahmad*, SCC, *supra* note 74.

125 *Charkaoui*, *supra* note 112.

126 *Canada (Citizenship and Immigration) v Harkat*, 2014 SCC 37.

removal to maltreatment – are more serious than anything that can be inflicted under the *Criminal Code*.[127]

Given this established caselaw, it would be the height of formalism to assume that just because the fruits of a warrant are being used in a criminal proceeding, a collateral *Garofoli* dispute over the CSIS warrant authorization process somehow attracts more rigorous open-court standards than does a proceeding on the *merits* that decides the fate of a person subject to a security certificate. If follows that the same legislated innovation that saves the security certificate regime under the *Charter* – special advocates – would also save a closed-court *Garafoli* proceeding involving CSIS intelligence.

A closed-court *Garafoli* proceeding might significantly reduce CSIS concerns about sharing the fruits of its warrants with the police, greatly increasing the information in zone AB.

E. Managing Public Safety

Even with all the innovations proposed above, there will be two investigations: the CSIS security intelligence investigation and the police criminal investigation. CSIS may have access to full information. The police may have access to somewhat less information, although ideally the steps noted above would ease information flows. In the hypothetical, who will decide that it is better to pick up Bob, Yves and Trent for conspiracy to commit to passport fraud rather than let the various investigations continue?

Even in systems, such as that in the United Kingdom where police and intelligence anti-terrorism investigations are more blended, there is need for a public safety fusion centre managing the public safety risk.[128] It is not clear to me how much of this "fusion" role is currently accomplished through CSIS/RCMP One Vision 2.0 collaboration. But I worry it is not fully possible to "fuse" where substantive information sharing from CSIS and RCMP is governed by carefully curated disclosure letters, and less regular, advisory letters. How can a fusion centre really operate if one player has full possession of the information, but the other does not?

My suspicion is, therefore, that our fusion centres could benefit from more fusion. A Canadian counterpart to the UK system could receive

---

127 *Charkaoui v Canada (Citizenship and Immigration)*, 2008 SCC 38 at para 54 ("The consequences of security certificates are often more severe than those of many criminal charges.")

128 See discussion in Forcese, *supra* note 5.

investigative information from all-of-government and be fully apprised of the public safety risks associated with an ongoing investigation (or parallel investigations). Since it would include representatives from all the services with legal powers to respond to threats, the full tool chest of legal options could be canvassed by the fusion centre in response to a public safety risk. The decision on whether to intervene, and how, would then be made based on full-information by this collaborative body, and not *de facto* taken by the entity with the most information because of siloed information collection. The interventions managed by this fusion body could be timed to minimize subsequent I2E dilemmas. For instance, arrests could be timed to support charges that requiring the least reliance on classified intelligence, while at the same time balancing the public safety interest.[129] (For example, in their original plot, Bob, Yves and Trent could be arrested while in possession of fake passports.)

The fusion centre would be structured to ensure it is not itself an investigative body or one that creates new information. Kept at arm's length in this manner, it would itself be a third-party to the criminal investigation and information in its possession would not be subject to more assertive disclosure obligations than already exist for CSIS under an *O'Connor* standard. In this manner, CSIS could collaborate with full information without exposing itself to disclosure obligations any greater than exist already.

Put simply: The fusion centre would be a black hole for in-bound information. And its contribution would be confined to making the decision on when to wrap up investigations and move against targets for urgent public safety reasons.

VII. Conclusion

In sum, I2E is a problem that can be managed, but the dilemmas cannot be outright solved. CSIS cannot wall itself off from the criminal justice system – at least, not without the enactment of a special, absolute privilege created using the "notwithstanding" clause of the *Charter*. (And were such a

---

[129] An attending police officer could plausibly point to the fusion centre tip-off as the basis of his or her reasonable and probable cause, even if the tip-off was not itself admissible evidence. *Eccles v Bourque*, *supra* note 49 at 746 ("That this information was hearsay does not exclude it from establishing probable cause" in an arrest context).

statute promulgated, I predict that courts would find other ways to invalidate trials made unfair by the privilege.)

But the disclosure risk can be managed, in a manner that threads the needle between fair trials, legitimate confidentiality concerns and public safety. This management system rests on three legs:

- Manage the relevance "tear-line" so that crimes are charged whose prosecution is less intrusive on CSIS information holdings. This strategy requires applying a prosecutorial insight to those investigations and planning their conduct to not prejudice trials. I bundle this concept within the category of "collecting to evidential standards" and "managing witnesses."
- Legislate standards to create certainty from the murk of evidence law. Here, two innovations stand out. First, legislate *O'Connor* style third-party status for CSIS where: CSIS's investigation is a *bona fide* security intelligence investigation; police do not have full, unmediated access to CSIS's files; and, CSIS does not take an active role in the police investigation. But do not build this legislated third-party status around rigid barriers on information-sharing. Second, legislate *ex parte, in camera* procedures for *Garofoli* challenges of CSIS warrants, substituting special advocates for defence counsel.
- Manage the public safety risk by creating a fusion centre able to receive investigative information from all-of-government and fully apprised of the public safety risks associated with an ongoing investigation (or parallel investigations). Ensure it includes representatives from all the services with legal powers to respond to threats. The fusion centre would not itself be an investigative body, and would have *O'Connor*-style third-party status, something that would not require legislation but which might benefit from it.

I suspect that these three steps would go a considerable distance to easing difficulties in the current conduct of Canadian anti-terrorism. It is true any new system will attract controversy and inevitable challenges by criminal defendants. That is the way the system is supposed to work. But the mere prospect of challenge should not deter, and I believe this system could be sustained. At any rate, the *status quo* has proven a magnet for challenges already, while contributing to a high-risk security environment.

Accordingly, from my (admittedly outsider) vantage point, I see no serious downside-risk to trying something different.