Navigating National Security: The Prosecution of the Toronto 18

CROFT MICHAELSON *

ABSTRACT

Prosecutions of terrorism cases pose unique challenges because they typically raise complex issues engaging the right of an accused person to disclosure of relevant material and the public interest in protecting national security. This chapter provides the lead prosecutor's perspective on the Toronto 18 prosecution, some of the disclosure issues that arose in that case, and how similar issues might be handled in the future. Part II provides an overview of the Toronto 18 investigation. Part III reviews the Canadian disclosure regime in the context of terrorism prosecutions, contrasts it with disclosure regimes in the U.K. and the U.S.A., and highlights some problems associated with the current bifurcated approach when the defence seeks to compel disclosure of sensitive information. Part IV discusses how the prosecution in the Toronto 18 approached the disclosure of information in CSIS holdings. Part V concludes with a discussion of how the prosecution managed its disclosure obligations in the context of the *Garofoli* review of the wiretap authorizations, and how similar issues might be handled in the future given subsequent developments in the law.

* Croft Michaelson, QC, formerly Senior General Counsel, Public Prosecution Service Canada, and lead prosecutor of the Toronto 18. I would like to thank Jason Wakely and George Dolhai for their comments on an earlier draft of this chapter – any errors that may remain are my own. The views expressed here are my own and not those of my former or current employers.

I. INTRODUCTION

The prosecution of the group that is commonly, and somewhat erroneously,[1] referred to as the Toronto 18 was a complex prosecution involving many difficult and unprecedented legal issues. The police investigation had its genesis in intelligence information provided by the Canadian Security Intelligence Service (CSIS), which was conducting a national security investigation against some of the individuals who became the subjects of the police investigation.

To give the reader some sense of the scope of the prosecution, the police investigation spanned approximately six months and involved two civilian agents, many investigators, authorizations to intercept communications, and search warrants, both covert and overt, which resulted in the generation of a voluminous amount of investigative material that was subject to disclosure and needed to be carefully reviewed to redact privileged information. The trial against the ten remaining adult offenders itself began with the assignment of the trial judge, Justice Fletcher Dawson, in late May 2008, who then promptly heard the first of approximately 30 pre-trial applications. Many of those applications were complex and involved novel legal questions relating to CSIS and its involvement in the investigation. By January 2010, four adult accused were left, the rest having pleaded guilty. Two trials then ensued – a judge-alone trial against one accused and a jury trial against three others. The judge-alone trial ended with a conviction in February 2010, and the jury returned guilty verdicts in late June 2010, more than two years after the trial had commenced.

---

1 The case is, perhaps, more accurately denoted the "Toronto 11", because although 18 individuals – 14 adults and four young persons – were initially charged, that number was ultimately reduced to 11 (ten adults and one young person). See the Introduction to this book for more details. Prosecutions may only be advanced by federal prosecutors if the evidence meets the test set out in the PPSC Deskbook; that is, the evidence must be sufficient to establish a reasonable prospect of conviction, and it must be in the public interest to proceed. The evidence is typically reassessed by prosecutors as the evidentiary landscape changes, such as after witnesses have testified at a preliminary hearing. Here, the Crown withdrew the charges against one adult accused and one young person was discharged after preliminary hearings. The Crown also stayed charges against three adults and two young persons, but those individuals consented to enter into judicial recognizances for one year under the predecessor provision to what is now s. 810.011 of the *Criminal Code*, R.S.C. 1985, c. C-46.

Any prosecution involving a lengthy police investigation and a large number of accused will inevitably be challenging for the prosecutors. Lengthy police investigations, particularly where the police have obtained authorizations to intercept communications and search warrants, typically generate large amounts of investigative material that can be difficult to manage and disclose in accordance with the Crown's duty to disclose the fruits of the investigation to the accused. Large numbers of accused persons also raise significant practical difficulties – few courtrooms are equipped for trials of more than a few individuals at a time; a jury may find it challenging to follow the evidence against more than seven or eight accused persons; in some cases, it may be almost impossible to craft intelligible jury instructions when a large number of individuals are prosecuted together and are facing complex charges.[2] The Toronto 18 prosecution was no different than many other cases in this respect. But what was unique about the Toronto 18 case was that, in addition to these commonplace challenges, the prosecution needed to also navigate its way through the national security interests that arose in the case. That is the basic theme of this chapter – a prosecutor's perspective on how we navigated our way through the national security issues that arose in the case and how those issues might be successfully navigated in the future. I also hope to show that although national security is uncommon and a rather esoteric subject matter in the context of criminal prosecutions, the issues that arise can be managed fairly in a manner that protects both national security and the right of an accused person to make full answer and defence. But in order to give context to what follows, I first begin with an overview of the investigation of the Toronto 18 and the national security issues that confronted the prosecution.

II. The Investigation of the Toronto 18

The police investigation of the Toronto 18 first began in November 2005 when CSIS sent the RCMP Integrated National Security Enforcement Team (INSET) in Toronto an "advisory letter"[3] detailing information that

---

2 For example, in R v. Pangman, 2000 MBQB 71, the court ordered severance where 15 accused were jointly charged on conspiracy and criminal organization charges, and the jury would have been required to return 84 discrete verdicts.

3 When intelligence information is shared between agencies, it is commonly subject to caveats restricting the use to which the information may be put, absent express approval from the agency providing the information. In this manner, agencies are able to control

CSIS had collected during its investigation of Fahim Ahmad, a young male who lived in the Toronto area. Although CSIS conducts investigations, it is not a law enforcement agency and has no mandate to investigate violations of the criminal law. CSIS is an intelligence service, the mandate of which was, in 2005, to collect information and intelligence relating to suspected threats to the security of Canada, and to provide reports and advice to the Government of Canada in respect of such threats.[4] The ability of CSIS to disclose information that it gathers during its intelligence investigations is governed by statute. When CSIS, in the course of a national security investigation, learns of criminal activity, CSIS may share that information with the police.[5] The police, in turn, can then initiate a criminal investigation and, ideally, arrest the offender(s). The extent to which intelligence information may be shared by CSIS will typically engage a balancing of the risks of compromising national security against the degree of the threat to public safety arising from the apparent criminal activity.[6] If

---

the use and dissemination of their information and thus mitigate risks that might arise from further disclosures of the information. CSIS provides both "advisory letters" and "disclosure letters" to the police; the terms used do not accurately describe – at least from the perspective of criminal practitioners – the nature of the documents. An "advisory letter", in the lexicon of CSIS, includes information that may be provided to an issuing justice for the purpose of obtaining judicial authorization to conduct a search or intercept communications, but it may not be further disclosed without the permission of CSIS. In contrast, a "disclosure letter" sets out information that the police may only use as an investigative lead – they cannot rely on any of the information as grounds for issuance of judicial process. In other words, none of the information in a "disclosure letter" may be disclosed beyond the recipient police force, but information in an "advisory letter" may be disclosed to an issuing justice.

4 Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23, s. 12. The mandate of CSIS was extended in 2015 to permit the Service to take measures to reduce threats to the security of Canada. See Canadian Security Intelligence Service Act, s. 12.1.

5 Generally speaking, CSIS is prohibited from disclosing any information that it collects, except in accordance with s 19 of the *Act*. Disclosure for the purpose of domestic law enforcement is one of the prescribed purposes; the Service may share information with peace officers and Attorneys General for the purpose of investigating and prosecuting contraventions of Canadian and provincial law. See Canadian Security Intelligence Service Act, s. 19(2)(a).

6 There are many ways that disclosing information may impact adversely on national security. For example, disclosure of the fact that information came from a human source may narrow the pool sufficiently to allow others to determine the identity of that source, endangering the source's safety – if source identities are not assiduously protected, persons will be reluctant to act as sources of intelligence in the future. Revealing sensitive information may reveal enough about the operations and capabilities of

death or serious bodily harm is likely to ensue from the criminal activity, there is a strong likelihood that CSIS will disclose the information to the police.

Fahim Ahmad had been on the radar screen of CSIS for some time when the first advisory letter was sent to INSET. He had been interviewed by CSIS in the spring of 2005. On one occasion in late June 2005, Ahmad and three of his associates were followed to a park by CSIS surveillance personnel. While Ahmad waited on the street, his associates went into a wooded area, a loud bang was heard, and the associates then rejoined Ahmad. In August 2005, two individuals connected to Ahmad – Ali Dirie and Yasin Mohamed – were stopped entering Canada from the United States by border security officers, as a result of a lookout that had been placed by CSIS with the Canadian Border Services Agency. When Dirie and Mohamed were searched, they were found in possession of handguns and ammunition that they were trying to smuggle into Canada; the vehicle they were driving had been rented with Ahmad's credit card.[7] INSET officers were informed of the arrests of Dirie and Mohamed but concluded, based on the information they then had, that there was no evidence that the smuggled firearms were intended for terrorist activity. Finally, in November

---

intelligence agencies to allow terrorist groups to frustrate or evade the interception of communications, hampering the ability of agencies to collect intelligence. Canada is also a net consumer of intelligence information obtained from its allies, meaning that we obtain more intelligence from our allies than we provide. Our relationships with our allies will likely suffer and they will be less likely to share sensitive intelligence information if Canada is not able to adequately safeguard that information. The balancing of the risk to national security posed by disclosure against the threat to public safety, therefore, will often dictate the degree of detail provided to the police and how the police may use that information.

7 Dirie and Mohamed both pleaded guilty to smuggling firearms and were sentenced to penitentiary terms of imprisonment. After the training camp, Ahmad sent extremist materials to Dirie in the penitentiary and had conversations with him concerning both the training camp and the acquisition of firearms. Dirie later pleaded guilty to participating in the activities of a terrorist group. When he was later released from prison, he entered into a judicial recognizance under s 810.011 of the *Criminal Code* (which is sometimes referred to colloquially as a "terrorism peace bond"). In any event, Dirie subsequently left the country in breach of the terms of his recognizance and travelled to Syria where he was reportedly killed in battle. See "'Toronto 18' member Ali Mohamed Dirie reportedly died in Syria," *CBC News*, September 25, 2013, https://www.cbc.ca/news/world/toronto-18-member-ali-mohamed-dirie-reportedlydied-in-syria-1.1868119.

2005, CSIS intercepted Ahmad's telephone conversations with another associate, in which they engaged in secretive discussions about meeting a contact in Pakistan.

By mid-November, the information collected by CSIS through its surveillance activities raised concerns within the Service that Ahmad and his associates posed a risk to public safety. Thus, on November 17, 2005, CSIS provided INSET investigators with an advisory letter summarizing some of the information that they had gathered relating to Ahmad and his activities.[8] The police then commenced their own criminal investigation on a parallel track.

The parallel nature of the CSIS and INSET investigations is illustrated by the events of November 27, 2005. By this date, INSET investigators were conducting surveillance on Ahmad and followed him to the Taj Banquet Hall, where Ahmad attended a public presentation on security certificates.[9] At the same time, CSIS asked one of their confidential human sources, Mubin Shaikh, to go to the banquet hall and see if he could manage to ingratiate himself with Fahim Ahmad, Zakaria Amara, and Amin Durrani.[10]

When Shaikh arrived at the banquet hall, he was able to join a table where Ahmad, Amara, and Durrani all sat. As the evening progressed, Shaikh was able to establish a rapport[11] with Ahmad and Amara, and they

---

8 Not all of the information collected by CSIS was shared; indeed, much was not. For example, CSIS held back the fact that they were aware that Ahmad had reacted with panic when he learned that Dirie and Mohamed had been arrested.

9 Under the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27, a security certificate may be issued by the government stating that an individual is inadmissible to Canada for reasons of national security, violation of human or international rights, or involvement in organized or serious crimes. Once signed, the certificate is referred to the Federal Court. If the Federal Court finds that the security certificate is reasonable, it becomes an enforceable removal order. A warrant may issue for the arrest and detention of a person named in a security certificate.

10 CSIS had obviously identified Amara and Durrani as associates of Ahmad by this point.

11 See Chapter 4 of this book for Shaikh's perspective on this dinner. Shaikh managed to present himself in a manner that made him an attractive target for recruitment: he was familiar with firearms through his past involvement with the army cadets, he had a firearms acquisition licence, and perhaps most importantly, he said that he believed that Jihad is an individual obligation (*fard al-ayn*), rather than a communal obligation (*fard al-kifayah*). Jihadist terrorist groups all invariably state that jihad is *fard al-ayn*. Although the term Jihad is subject to various interpretations within Islam, for the purposes of this chapter I adopt the meaning used by Islamist terrorist groups – fighting in the cause of Allah or, in other words, violent acts committed for a religious objective or purpose. This interpretation of the term Jihad is not restricted to terrorist groups;

tried to recruit Shaikh to join a group they were forming to carry out terrorist acts. Ahmad explained that he wanted to launch attacks on critical infrastructure targets in Canada and invited Shaikh to attend a training camp in December in a rural area north of Toronto. At one point during the evening, Amara reached inside his jacket, disengaged the magazine for a handgun, and showed it to Shaikh. Referring to the bullets inside the magazine, Amara said, "these are cop killers." When the evening wrapped up, police surveillance officers followed Ahmad but did not follow Amara because they had not yet identified him as a person of interest. CSIS surveillance personnel, therefore, picked up the surveillance of Amara once he left Ahmad's presence.

In a subsequent meeting that occurred a couple of days later, Ahmad told Shaikh his intended targets – Parliament, power grids, the nuclear power station in Pickering, and military sites. Ahmad said that he had a cache of weapons that he had buried in a park. He also told Shaikh that he had sent a couple of guys to the United States to bring back some weapons, but they had been caught and arrested at the border. Ahmad asked Shaikh, who Ahmad knew to have once been an army cadet rifle instructor, to help him train the recruits who attended the training camp.

The information gathered by Shaikh, which now indicated that Ahmad had identified specific targets, resulted in CSIS providing another advisory letter to the police. When the police received this letter, they decided that they would need to rely on the contents of the advisory letters as grounds to obtain authorization to intercept Ahmad's communications, but before doing so, they sought further detail from CSIS about the source(s) of the information.[12] CSIS then decided to see if Shaikh was willing to become a

---

one widely distributed English translation of the Holy Quran, published by the Saudi Arabian government, adopts the same interpretation. See Taqi Ud Din Hilali and Muhammad Muhsin Khan, *Translation of the Meanings of The Noble Qur'an in the English Language* (Saudi Arabia: King Fahd Complex for the Printing of the Holy Qur'an, 2006), Glossary, definition of *Jihad*.

12 It is well established that the determination of whether informer information is reliable requires an assessment of the following factors: the compelling nature of the information, the credibility of the source, and the extent to which the information has been corroborated. Weaknesses in one area may be compensated by strengths in the other. See R v. Debot, [1989] 2 S.C.R. 1140, 37 O.A.C. 1, per Justice Wilson. The INSET investigators, therefore, sought additional information relating to the source or sources of the CSIS information so that the investigators (and any issuing justice) could determine whether that information was reliable.

police informer; when Shaikh indicated that he was, he was handed over to the police. Shaikh then became a confidential police informant entitled to the traditional common law protection afforded to police informers, whose identities may only be disclosed if it is necessary to prove the factual innocence of an accused person.[13] When Shaikh was debriefed by a source handler for the police, Shaikh essentially repeated the information that he had previously provided to CSIS about Ahmad and his plans. The information gathered by the source handler from Shaikh, along with the information provided in the CSIS advisory letters, became the foundational grounds for an application under Part VI of the *Criminal Code* to intercept the communications of Fahim Ahmad, Zakaria Amara, and their associates.[14]

Shaikh subsequently agreed to attend Ahmad's training camp, which was held at a remote location north of Orillia, Ontario, in late December. The police were able to intercept some of Ahmad's cell phone communications during the training camp, but much of the information about what took place at the camp – firearms training, simulated military-type exercises, and lectures on Jihad – and who did what was initially provided to the police by Shaikh and corroborated through subsequent seizures of evidence.[15]

Recognizing that Shaikh's evidence would be helpful in any future prosecution, the police had asked Shaikh if he would be prepared to waive his status as a police informant and become a police agent, which would mean the eventual disclosure of his identity and that he testify at trial. Several weeks after the training camp, Shaikh agreed to do so.[16]

---

13 R v. Leipert, [1997] 1 S.C.R. 281, 143 D.L.R. (4th) 38; R v. Basi, 2009 SCC 52; Named Person v. Vancouver Sun, 2007 SCC 43.

14 R v. Ahmad, [2009] O.J. No. 6162.

15 Subsequent computer searches revealed video footage of a lecture given by Ahmad at the camp, which amply described the terrorist purposes of the group. Another video surfaced much later on the Internet depicting some of the firearms training, marching, and quasi-military exercises that were held during the camp. This particular video had an interesting backstory – it was originally seized from an individual who was charged with terrorism-related offences in the United Kingdom. It was posted online by the NEFA foundation after it was played at the trial of the accused in the U.K. It would seem that that individual received the video from Ahmad, who was intercepted by the police on one occasion advising Amara that he had shown the video to another individual who had been impressed.

16 R v. N.Y., 2008 CanLII 51935 (ON SC).

The police investigation of Ahmad, Amara, and the other camp attendees continued – communications were intercepted, surveillance was conducted, and Shaikh continued to gather evidence. However, Amara grew frustrated with Ahmad, severed his ties with the group, and recruited Shareef Abdelhaleem, Saad Khalid, and Saad Gaya to join him in a conspiracy to bomb targets in downtown Toronto and elsewhere in Ontario.[17]

Fortunately, a friend of Abdelhaleem, Shaher Elsohemy, had been recruited as a human source by CSIS. Elsohemy was eventually introduced to Amara by Abdelhaleem and was taken into their confidence. In particular, on April 8, 2006, Amara expressed an interest in acquiring large quantities of ammonium nitrate[18] and revealed his plan to bomb three targets. This information was promptly passed on to the police by CSIS, and four days later, Elsohemy became a police informer. In the ensuing weeks, Elsohemy had discussions with Abdelhaleem and Amara about the bomb plot and provided a great deal of helpful information to the police, but because Elsohemy was an informer, none of that information could be used as evidence at trial. The police, therefore, sought to have Elsohemy become a police agent and, on May 10, 2006, Elsohemy agreed to do so. The police then obtained authorization to intercept communications, and, from that point on, Elsohemy's conversations with Abdelhaleem and Amara about the bomb plot were intercepted and recorded.[19]

Abdelhaleem and Amara placed an order for three tonnes of ammonium nitrate with Elsohemy. In the meantime, police surveillance officers recorded Amara meeting with Khalid and Gaya at McMaster

---

17 Amara's targets were the CSIS regional office and the Toronto Stock Exchange in downtown Toronto, as well as an unidentified military base. Unbeknownst to Amara and his co-conspirators, the offices of the Department of Justice and the Public Prosecution Service of Canada would have been collateral targets if the bombings were carried out, because both offices were located in the same building as the TSX.

18 Ammonium nitrate is the main component of a fertilizer bomb, such as was used in the bombing of the federal building in Oklahoma City. Amara's plan was to build three bombs, each containing one tonne of ammonium nitrate. In order to establish the explosive force of such a bomb, the INSET investigators had a similar bomb constructed and detonated under scientific conditions. The expert report established that a bomb made of one tonne of ammonium nitrate would cause death and serious bodily harm to persons in the vicinity of the explosion and cause serious damage to an office building.

19 R v. Abdelhaleem, [2010] O.J. No. 5693.

University and having a discussion, during which Amara made a hand gesture of detonating a bomb. On June 2, 2006, undercover officers delivered three tonnes of an inert substance packaged as ammonium nitrate to a warehouse that Abdelhaleem had rented. Khalid and Gaya, wearing t-shirts with the logo "Student Farmers,"[20] were recorded unloading much of the "ammonium nitrate" until they, and all of the other individuals who comprised the Toronto 18, were arrested and charged with terrorism-related offences. The case then moved to the prosecution phase.

As mentioned in the introduction to this chapter, the Toronto 18 case posed the usual difficulties for the prosecution that can arise in any lengthy wiretap investigation of multiple accused persons. Managing and vetting voluminous disclosure materials; reviewing extensive evidence to ensure that the standard for initiating a prosecution is met for each individual accused and that the appropriate charges have been laid; determining whether and how to sever accused persons, so the Crown can present a coherent and manageable case at trial; and responding to the inevitable attacks on the admissibility of seized evidence are routine challenges that confront prosecutors who deal with complex investigations of criminal organizations. But overlaying those routine challenges were two that were unique to this particular prosecution and arose from the intersection of CSIS and national security interests with the police investigation.

The first challenge arose in the context of the Crown's disclosure obligation: to what extent, if any, did the involvement of CSIS impact the Crown's obligation to disclose information to the accused? The second challenge arose in the context of the review of the initial authorization to intercept communications: if the police relied on information provided by CSIS as grounds to obtain an authorization to intercept communications, how does this impact the review of that authorization, and what are the implications for disclosure? In what follows, I will discuss how we dealt with these issues in the prosecution of the Toronto 18 but also suggest how such issues might be dealt with in the future given more recent developments in the case law.

---

[20] The logo would seem to have been intended to explain to any passers-by why they were handling a large quantity of ammonium nitrate, a fertilizer.

III. Navigating National Security – Disclosure of the Fruits of the Investigation

It has been well established, since the decision of the Supreme Court of Canada in *R v. Stinchcombe*, that the accused's constitutional right to make full answer and defence under section 7 of the *Charter of Rights and Freedoms* imposes a duty on the Crown prosecutor to disclose relevant information in their possession or control, unless the information is privileged.[21] This duty to disclose includes both inculpatory and exculpatory information.[22] Information is relevant in the context of disclosure if it can reasonably be used by the accused to meet the case for the Crown, advance a defence, or otherwise make a decision that could affect the conduct of the defence.[23]

Because the Crown obtains the materials for use in a prosecution from the police, and the right to disclosure would be a hollow one if the police could cherry-pick what they give to the Crown, the police have a corollary duty to provide the prosecutor with "all material pertaining to the investigation of the accused."[24] This corollary duty encompasses the "fruits of the investigation" – the material created or acquired by the police in the course of their investigation – but it also includes any other information

---

21 R v. Stinchcombe, [1991] 3 S.C.R. 326, [1992] 1 W.W.R. 97; R v. Gubbins, 2018 SCC 44; R v. Quesnelle, 2014 SCC 46; R v. McNeil, 2009 SCC 3.

22 *Stinchcombe*, S.C.R.; *Gubbins*, SCC at para 22.

23 *Gubbins*, SCC at para 18; R v. McQuaid, [1998] 1 S.C.R. 244 at paras 20–22, 37 W.C.B. (2d) 204. The requirement that information be disclosed if it could be used to "make a decision which could have affected the conduct of the defence" has the potential to denude relevancy of meaning if it is interpreted too broadly. One could argue that the defence needs disclosure of everything in the investigative file in order to ensure that they have advanced all possible pre-trial motions and applications. For example, if none of the non-disclosed information in an investigative file could reasonably support an application for abuse of process, the defence might still argue that they require production of the material so they can decide that an abuse of process application is without merit. Pushed to absurdity, the defence could argue that they require production of all of the irrelevant information because it would help them make a decision as to whether the Crown has withheld relevant or irrelevant information. Information that is irrelevant becomes "relevant" because the defence would see that it is irrelevant. It seems that when the court made the reference to decisions affecting the conduct of the defence, it was referring to tactical decisions at trial, such as whether the accused should testify, or whether certain evidence should be called or admitted.

24 *McNeil*, SCC at paras 23, 52.

that is "obviously relevant to the accused's case," such as the criminal record of a witness.[25]

The prosecutor's duties in respect of disclosure can reach beyond the *Stinchcombe* disclosure obligation and the "fruits of the investigation" and "obviously relevant" information in the hands of the investigative agency. If the prosecutor has reason to believe that another government agency is likely in possession of information that is relevant to the defence of the accused, the prosecutor has a duty, under *R v. McNeil*,[26] to request that information from the agency. This duty to seek out information from third-party government agencies is referred to as the "*McNeil* duty." If the prosecutor is provided with the information, then the *Stinchcombe* standard of relevance applies. If, however, the agency refuses to provide the information, the defence is required to bring an application for production from a third party, the standard for which was laid down by the Supreme Court in *R v. O'Connor*.[27] I discuss the *McNeil* duty and its application in the context of the Toronto 18 prosecution in Part IV below.

The Crown prosecutor's duty to disclose is a broad one. Prosecutors are required to err in favour of inclusion and may only withhold information that is "clearly irrelevant," privileged, or subject to some other legislative regime governing disclosure.[28] The disclosure obligation essentially operates as a form of open discovery of the investigative file and seems to be grounded in the rationale that records created during the investigation are presumptively relevant to the prosecution and defence of the offence charged.[29]

While the underlying rationale for the broad disclosure obligation – that investigative materials are presumptively relevant to the trial of the offence charged – may be well-founded in the context of routine criminal investigations, it begins to lose its force as the length and complexity of an investigation increase. Anyone who has prosecuted an offence that came

---

25 *McNeil*, SCC at para 59; *Gubbins*, SCC at para 23. The criminal record of a witness is relevant to an accused's case because such records can be used to impeach the witness at trial. See David M. Paciocco and Lee Stuesser, *The Law of Evidence*, 6th ed. (Toronto: Irwin Law, 2011), 448.

26 *McNeil*, SCC.

27 R v. O'Connor, [1995] 4 S.C.R. 411, 130 D.L.R. (4th) 235.

28 *McNeil*, SCC at para 18. For example, the disclosure of medical and therapeutic records of complainants in sexual assault trials is governed by ss. 278.1-278.91 of the *Criminal Code*.

29 *Quesnelle,* SCC at para 56.

out of a long, complex investigation can attest that much of the investigative file is completely irrelevant to the issues at trial. Much of what investigators generate during an investigation is more aptly described not as "fruits," but as withered buds on the vine. During a lengthy investigation, extensive surveillance may be conducted, much of which reveals nothing going towards guilt or innocence; myriad communications may be intercepted, furnishing nothing of evidentiary value; administrative documents may be created seeking approval for overtime or travel; and potential avenues of investigation may arise and be pursued until the investigators realize they are blind alleys. By way of example, during the investigation of the Toronto 18, investigators conducted routine surveillance on the subjects of the investigation. If a subject was seen waving or talking to someone in the parking lot of a mosque after prayers, surveillance officers would often note down the licence plate of that person for follow-up. Investigators would then conduct background enquiries of the person on police databases and open sources on the Internet – such enquiries typically were dead-ends and resulted in nothing that could assist the defence at trial.

In a lengthy and complex investigation, in which there are large quantities of material irrelevant to the prosecution of the offence, the task of culling through the investigative file to remove the information that is "clearly irrelevant" can pose a significant burden if the Crown takes seriously its obligation to "sort the wheat from the chaff."[30] And if information in the file materials is privileged, the burden is only magnified. In the "Toronto 18 case," the review and vetting of file materials for disclosure was laborious and spanned many months. Every investigator is required to make notes during an investigation, and a significant portion of the disclosure materials consisted of such notes. An investigator's notes are typically handwritten. They include notations of the investigator's personal observations and activities, but they will also commonly record information that is conveyed to the investigator by another investigator. For example, if a group of investigators attend a meeting where they obtain a debriefing on recent developments in the investigation, each investigator may well record that information in their notebooks. There will often be considerable overlap and duplication of information in the investigators' notes.

When sensitive, privileged information is shared among investigators during the investigation, a careful review of the notes is, therefore, required

---

[30] *Stinchcombe*, S.C.R. at 339.

in order to ensure that none of the privileged information is buried in someone's notes and inadvertently disclosed. The fact that the notes are commonly handwritten further complicates matters because, unlike the electronic text generated by word processing software programs, handwriting is highly variable among writers, and OCR software[31] cannot be used to search handwritten notations with any degree of certainty. In the Toronto 18 investigation, it was not uncommon for privileged information provided by CSIS to be shared among members of the investigative team. It was, therefore, necessary to engage in a line-by-line, page-by-page review of every investigator's notes to ensure that the information was redacted from the notebooks before they were disclosed to the defence. And because CSIS had a direct interest in the privileged information, CSIS needed to be provided with an opportunity to review the notations to verify that none of their sensitive information would be disclosed inadvertently.

In order to comply with its disclosure obligation in a timely manner, the Crown disclosed the relevant, non-privileged material in an electronic format in successive waves. The initial wave consisted of bail packages and the affidavits used to obtain authorizations to intercept communications and search warrants. Because those affidavits set out a detailed chronology of the investigation, the defence were able to quickly get up to speed on the nature of the allegations against the accused. Subsequent waves of disclosure were concerned with seized evidence, officer notes, surveillance reports, and other documentation generated by the police during the investigation. The bulk of disclosure was provided to defence counsel within six months of the arrests, and disclosure was essentially completed within ten months. To give some sense of the magnitude of disclosure in the case, at one point the disclosure provided to the accused consisted of more than 90,000 records, 82,000 text files of monitors' summaries of intercepted communications, and many media files.[32] After review by the police and CSIS, the Crown applied more than 9,600 redactions to these disclosure materials.[33] The redactions related to information that was subject to claims of privilege or public interest immunity – information that would reveal investigative techniques, the personal information of innocent third parties, or

---

31 Optical Character Recognition (OCR) software is not currently sophisticated enough to consistently identity words that have been handwritten in cursive writing. Indeed, many human readers struggle to interpret the cursive handwriting of others.

32 R v. Ahmad, 2009 CanLII 84788 at para 3, 257 CCC (3d) 135 (ON SC).

33 R v. Ahmad, [2009] O.J. No. 6152 at para 2 [*Ahmad* 2009].

information that would compromise national security – as well as information that was clearly irrelevant.

The broad, common law disclosure regime in Canada does not allow for any consideration of proportionality or any assessment of the extent to which information is material to the determination of issues at trial. Information within the investigative file must be disclosed if there is a "reasonable possibility that it may assist" the accused in making full answer and defence, unless it is privileged or subject to some other statutory disclosure regime.[34] Although burdensome, our disclosure regime is arguably not that different than the regimes in other common law countries, and placing a broad disclosure obligation on the Crown is probably the safest way to guard against wrongful convictions and miscarriages of justice.

In the United Kingdom, the prosecution is required to disclose to the defence any material that they intend to rely on at trial, what is commonly referred to as "used material." But the prosecution is also required to disclose any other material relating to the investigation that "might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused" (commonly referred to as "unused material").[35] This standard for disclosure is not much different than the *Stinchcombe* standard. I doubt that there is much difference in practice between a regime that requires the disclosure of information if "there is a reasonable possibility that it may assist" the accused and a regime that requires the disclosure of information that "might reasonably be considered capable… of assisting the case for the accused." Just as Canadian prosecutors have been instructed to err in favour of inclusion,[36] prosecutors in the United Kingdom have been told, "if in doubt, disclose."[37] If disclosure in Canadian criminal proceedings happens

---

34 *McNeil*, SCC at para 17.

35 Criminal Procedure and Investigations Act 1996 (U.K.), 1996, s. 3.

36 *Stinchcombe*, S.C.R. at 339.

37 U.K., HC, *Mouncher Investigation Report* (Cm 292, 2017) at 225 (Richard Horwell), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/629725.pdf; U.K. Attorney General's Office, Review of the Efficiency and Effectiveness of Disclosure in the Criminal Justice System (Cm 9735, 2018) at 12, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/Attorney_General_s_Disclosure_Review]. The U.K. disclosure regime in its application has been the subject of repeated criticism and resulted in enough miscarriages of justice that it is doubtful that that regime is an improvement over the

to be broader than in the United Kingdom, that probably follows from the fact that investigations in Canada are subject to greater scrutiny under the *Charter of Rights and Freedoms*. Simply put, more avenues are available to the defence in Canada to challenge the conduct of the police and make full answer and defence, and thus, more information within the investigative file is potentially relevant to triable issues and must be disclosed.[38]

Disclosure in federal criminal trials in the United States is governed by a mix of constitutional law and rules of procedure. Under *Brady v. Maryland*,[39] a violation of the due process clause of the 14th Amendment will arise whenever the prosecution withholds evidence that is favourable to the accused and "material either to guilt or punishment." This includes both exculpatory material and material that could be used to impeach key government witnesses.[40] Evidence is material in the *Brady* context if "its suppression undermines confidence in the outcome of the trial."[41] That is, there must be "a reasonable probability that, had the evidence been disclosed to the defence, the result of the proceeding would have been different."[42]

Under Rule 16 of the *Federal Rules of Criminal Procedure*, the government must, on the defendant's request, disclose any relevant written or recorded statement of the defendant if: (1) the statement is within the government's

---

Stinchcombe regime. See U.K., HC, *Disclosure of Evidence in Criminal Cases* (Cm 859, 2018) at 10–12, https://publications.parliament.uk/pa/cm201719/cmselect/cmjust/859/859.pdf.

38 A simple example will suffice to illustrate the point. In Canada, evidence that was seized illegally is an infringement of s. 8 of the *Charter* and is subject to exclusion if the admission of the evidence would bring the administration of justice into disrepute. In contrast, in England and Wales, any evidence that is relevant is admissible in criminal proceedings even if it was obtained illegally by the police, although the trial judge has a discretion to exclude evidence that would result in an unfair trial. See Public Prosecution Service v. McKee, [2013] UKSC 32 at para 9; Police and Criminal Evidence Act 1984 (U.K.), s. 78. Apart from statements, the admission of relevant evidence that was obtained illegally will only rarely have an adverse impact on trial fairness. Thus, an illegal seizure of evidence in Canada gives rise to a triable issue, while the same illegal seizure in the U.K. typically will not lead to a triable issue. In the result, the Canadian prosecutor will need to disclose more information that the U.K. prosecutor, but this arises from the nature of the justiciable legal issues in each jurisdiction, rather than meaningful differences in the disclosure regimes.

39 373 U.S. 83 (1963).

40 Giglio v. United States, 405 U.S. 150 (1972).

41 United States v. Bagley, 473 U.S. 667 (1985) at 678.

42 *Bagley*, U.S. at 682.

possession, custody, or control and (2) the attorney for the government knows, or through due diligence could know, that the statement exists. The government must also, on the defendant's request, permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and (1) the item is material to preparing the defence; (2) the government intends to use the item in its case-in-chief at trial; or (3) the item was obtained from or belongs to the defendant.[43]

In some respects, the disclosure obligation in the United States is narrower than in Canada. Under *Brady*, the failure to disclose information will only result in a due process violation if it is reasonably probable that the information would have affected the outcome at trial. In determining whether information needs to be disclosed, a federal prosecutor in the United States, therefore, must assess the probability that the information will assist the defence at trial, either in undermining the prosecution's case, advancing a defence, or mitigating a sentence. This can be a daunting exercise, particularly when the information is not clearly irrelevant to issues that may determine guilt or innocence or the imposition of sentence. As a prosecutor, do you take the risk that a guilty verdict or sentence will be overturned because you held back information that might have assisted the defence?

It is perhaps not surprising then that, as a matter of policy, U.S. federal prosecutors are encouraged to provide disclosure to the defence that goes beyond the *Brady* requirements. U.S. federal prosecutors are instructed as a matter of policy "to err on the side of disclosure in close questions of materiality."[44] Moreover, prosecutors are encouraged to disclose "relevant exculpatory or impeachment information that is significantly probative of the issues before the court but that may not, on its own, result in an

---

43 *Federal Rules of Criminal Procedure*, 2021 ed. (Michigan: Michigan Legal Publishing Ltd, 2020), Rules 16 (a)(1)(B), (E). If the defence makes a request under Rule 16(a)(1)(E), it triggers reciprocal disclosure on the part of the defence (see Rule 16(b)(1)). Under both the *Jencks Act*, 18 U.S.C. § 3500 and Rule 26.2, after a witness for the government has testified in-chief, the government is also required to disclose the statement of a witness relating to the subject matter of the testimony.

44 U.S., Department of Justice, *Justice Manual* (Washington, D.C.: U.S. DOJ, 2018), s. 9-5.001 C., https://www.justice.gov/jm/jm-9-5000-issues-related-trials-and-other-court-proceedings.

acquittal or, as is often colloquially expressed, make the difference between guilt and innocence."[45] This requires that prosecutors "disclose information that is inconsistent with any element of any crime charged against the defendant or that establishes a recognized affirmative defense" and "information that either casts a substantial doubt upon the accuracy of any evidence the prosecutor intends to rely on... or might have a significant bearing on the admissibility of prosecution evidence," regardless of whether the prosecutor believes that the information will make the difference between conviction and acquittal.[46] But this is still a narrower standard than the *Stinchcombe* disclosure obligation, which requires that prosecutors disclose information that is of only marginal relevance to issues at trial.

The breadth of the *Stinchcombe* obligation in the context of a complex, lengthy investigation with significant privilege issues imposes an onerous burden on the prosecution. No doubt other equally effective disclosure regimes could be crafted, but the *Stinchcombe* standard at least has the benefit of providing clear guidance to prosecutors. It is relatively easy to identify information that is clearly irrelevant – it simply involves asking whether the defence could use the information in any way to undermine the Crown's case, lay the groundwork for a defence, or decide how to conduct the trial. A broad, clear standard for disclosure also has the advantage of protecting against wrongful convictions. If prosecutors are not required to make the judgment call as to whether the defence will be able to successfully use the information and are simply required to determine whether the information may reasonably assist the defence, there is less likelihood of error.

Generally speaking, whenever the prosecutor has redacted information on the basis of privilege or irrelevancy, the defence can ask the trial judge to review the prosecutor's decision.[47] If the judge finds that the redaction was not justified or was too broad, the judge will order that the redaction be lifted or varied. In most cases, responsible defence lawyers will be content with the Crown's redactions, provided that they are aware of the general

---

45 U.S. Department of Justice, *Justice Manual*, s. 9-5.001 C.

46 U.S. Department of Justice, *Justice Manual*, s. 9-5.001 C.

47 *Stinchcombe*, S.C.R. at 340–41. In *Stinchcombe*, Justice Sopinka stated, at p. 340, that the trial judge on a review should be guided by the general principle that, unless information it privileged, information should not be withheld if there is a reasonable possibility that withholding the information will impair the accused's right to make full answer and defence.

reasons why the information is being withheld. In federal prosecutions, prosecutors typically tag each redaction with a code that informs the reader what the basis was for the redaction. For example, a redaction might be coded as "investigative technique," "solicitor-client privilege," "informer privilege," or "irrelevant." If information has been withheld as "irrelevant," prosecutors will often provide some additional information explaining why they say it is irrelevant, such as "unrelated investigation."

In theory, though, an accused person could ask the trial judge to review every single redaction made in disclosure materials. Indeed, that position was initially advanced by one of the counsel in the Toronto 18. As one might expect, the suggestion that the judge embark on a review of 9,600 redactions in thousands of pages of disclosure did not meet with a friendly reception, and Justice Dawson instructed the defence to meet with the Crown to narrow the scope of what he needed to review. After the Crown and defence met, the number of redactions for review was reduced significantly, and the review was completed in only a couple of days.[48]

When a redaction is made on the basis of national security privilege[49] – the claim that disclosure would cause injury to national security – an additional layer of complexity is added. This is because such claims have the potential to engage sections 38 to 38.14 of the *Canada Evidence Act* (*CEA*), which essentially provide that national security privilege claims may only be reviewed and set aside by a designated judge of the Federal Court of Canada. In other words, section 38 results in the bifurcation of jurisdiction relating to the review of Crown disclosure decisions. The trial judge has jurisdiction to review all Crown redactions in the disclosure materials, except those made on the basis of national security privilege; only the Federal Court has jurisdiction to review the latter and order disclosure. To better understand how the section 38 regime may become engaged in criminal trial proceedings and the difficulties it raises from a prosecutor's perspective, it is necessary to briefly review these provisions.

---

48 *Ahmad* 2009, O.J. at paras 1–3.

49 I use the term "national security privilege" for ease of reference. The Supreme Court of Canada stated in Carey v. Ontario, [1986] 2 S.C.R. 637 at 653, 35 D.L.R. (4th) 161, that Crown privileges are more properly described as "public interest immunities." A public interest immunity involves the balancing of public interests and will arise whenever the public interest in non-disclosure of information outweighs the public interest in disclosure.

A. The Section 38 Regime

The section 38 regime in the *CEA* basically codifies the common law of public interest immunity in relation to national security, national defence, or international relations. The regime applies to both "potentially injurious" and "sensitive" information. As defined in the *CEA*, "potentially injurious" information means any information that could injure national security, national defence, or international relations if it is publicly disclosed; "sensitive" information means information relating to national security, national defence, or international relations that is in the possession of the Government of Canada, and that the Government of Canada is taking measures to safeguard.[50]

The regime is applicable to both criminal and civil proceedings. Under section 38.01 of the *CEA*, any person who, in connection with a proceeding, is required to disclose, or who expects to disclose or to cause the disclosure of, potentially injurious or sensitive information is required to give written notice to the Attorney General of Canada of the possibility of the disclosure. Notice is not, however, required if the government department or agency that is the owner of the information authorizes disclosure.[51]

Stated differently, the section 38 regime is intended to protect classified information from unnecessary disclosure in the context of criminal or civil proceedings. In the Toronto 18 case, information in the investigative file relating to national security was uniformly classified as "Top Secret."[52] In some instances, the RCMP was the "owner" of the classified information because the RCMP had produced the information or had received it from a non-government entity. In other instances, CSIS was the "owner" of the information. Either agency could authorize the disclosure of their own

---

50 Redactions based on claims that disclosure would cause injury to national defence or international relations are less common in the criminal prosecution context, but that is not to say that they never arise.

51 Canada Evidence Act, R.S.C. 1985, c. C-5, s. 38.01(6)(c).

52 Information is classified according to the extent of injury to the national interest that would be caused if the information were disclosed. If disclosure would cause "injury" to the national interest, the information should be classified as "Confidential". If disclosure would result in "serious injury", the information should be classified "Secret". "Extremely grave injury" to the national interest requires a "Top Secret" classification. In my experience, information that triggers national security privilege is invariably classified as "Top Secret".

information by declassifying that information – this in fact occurred in respect of some material that had been originally classified as "Top Secret" during the investigation.[53] But where disclosure was not authorized by the agencies, if the defence wished to cause the disclosure of the information, or if the prosecutor was required to disclose the information, written notice to the Attorney General of Canada was required under section 38.01.

In general terms, if notice is given under section 38.01, disclosure of the information that is the subject of the notice is prohibited unless the Attorney General or a designated judge of the Federal Court subsequently authorizes disclosure.[54] Under subsection 38.03(1) of the *CEA*, the Attorney General may, at any time and subject to any conditions, authorize the disclosure of all or part of the classified information. The Attorney General is required to advise the person who provided the written notice of the Attorney General's decision with respect to disclosure within ten days.[55] If the Attorney General does not provide notice of a decision, or makes any decision other than authorizing full disclosure of the information without conditions, the person who wishes to disclose, or to cause the disclosure, of the information may apply, under paragraph 38.04(2)(c), to the Federal Court for an order in respect of disclosure. A person who is required to disclose information, other than a witness, must apply to the Federal Court under paragraph 38.04(2)(b) for an order.[56]

In other words, whenever an accused person wishes to cause the disclosure of classified information in a criminal proceeding and gives notice to that effect to the Attorney General, the accused may then bring an application in Federal Court for disclosure if the Attorney General has not authorized the disclosure of the information, in its entirety and without conditions, within ten days.[57] If a prosecutor is required to disclose classified

---

53 Everything relating to a national security investigation will ordinarily be classified as "Top Secret" during the investigation because disclosure would compromise the investigation. But once the investigation is completed and arrests are made, that particular concern usually dissipates.

54 Canada Evidence Act, s. 38.02(2).

55 Canada Evidence Act, s. 38.02(3).

56 If a witness is required to disclose, or wishes to disclose, classified information and serves notice, the Attorney General is required to bring an application in Federal Court in respect of disclosure.

57 Unless the accused and the Attorney General have entered into a disclosure agreement under s. 38.031 of the *Canada Evidence Act*, something I have yet to see used in criminal proceedings.

information and gives notice, the prosecutor must bring an application in Federal Court for an order in respect of disclosure when the Attorney General does not authorize the disclosure of the information, in its entirety and without conditions, within ten days.

The Federal Court judge hearing the application in respect of disclosure may authorize disclosure of the information if the judge concludes that disclosure would not injure national security (or national defence or international relations).[58] If the judge concludes that injury to national security would ensue, the judge may only authorize disclosure of classified information where the public interest in disclosure outweighs the public interest in non-disclosure.[59] The judge must consider if there are ways to limit the injury to national security, such as by imposing conditions on disclosure or by ordering that only a summary of the information or written admission of facts be disclosed.[60]

As stated above, in the Toronto 18 case, some information that, if disclosed, would have caused injury to national security was included within the materials that had been generated or obtained by the police during the investigation. The information was redacted from the disclosure materials and withheld on the basis of a national security privilege. In accordance with a practice that first arose in *R v. Khawaja*, the prosecution served a section 38.01 notice on the Attorney General of Canada.[61] This particular practice has been followed in the years since, but on reflection, I think that the practice of the prosecutor giving notice rests on a misreading of section 38.01 and *R v. Stinchcombe*.

Section 38.01 only requires notice if a party to a proceeding is required to disclose, or expects to disclose or to cause the disclosure of, classified information. Nothing in the Crown's *Stinchcombe* disclosure obligation requires that the prosecutor disclose information that is subject to a privilege or public interest immunity. To the contrary, *Stinchcombe* recognizes that information may properly be withheld if it is subject to privilege. When we redacted information from the investigative file materials, we were asserting a public interest immunity. We were not required to disclose the information and had no intention of disclosing the

---

58 Canada Evidence Act, s. 38.06(1).

59 Canada Evidence Act, s. 38.06(2).

60 Canada Evidence Act, s. 38.06(2).

61 For the procedural history of the s. 38 hearing in *R v. Khawaja*, see Canada (Attorney General) v. Khawaja, 2007 FC 490 at paras 11, 15, 31–34.

information or causing its disclosure. In hindsight, the accused were required to give notice under section 38.01 because they were the persons seeking to challenge the redactions and, therefore, the persons who expected to cause the disclosure of the redacted information in the criminal trial proceeding.

The practice of the prosecutor giving routine notice whenever sensitive or potentially injurious information is redacted from disclosure materials is problematic and should be avoided in the future. Once the notice is served, the section 38 process is triggered. That process inevitably results in a time-consuming and costly application to the Federal Court for an order in respect of disclosure. But much of the information that is redacted on the basis of national security privilege is only marginally relevant, at best. Left to their own devices, many defence counsel might well decide not to go behind any of the redactions, or to just try to do so in respect of a limited number of them. That is often what transpires in criminal trials – the defence accepts that the Crown discharged its disclosure obligations in a responsible manner and does not ask the trial judge to review redactions made on the basis of informer privilege or solicitor-client privilege. The only time that a prosecutor should serve a section 38.01 notice is when the prosecutor has been ordered to disclose the information by the trial court, or when the prosecution reasonably expects to disclose the information to the trial judge in the course of the trial proceedings.[62]

Even though a section 38.01 notice was served in the Toronto 18 prosecution, no Federal Court hearing was ever conducted. The reason for that was that the trial judge held that the section 38 regime was

---

[62] Situations will likely arise where the prosecutor can reasonably expect that disclosure of sensitive information will be required during the trial proceedings to the trial judge. For example, in the context of a *Garofoli* review of a wiretap affidavit (discussed below), a prosecutor may ask the trial judge to consider information in the affidavit that has been withheld from the defence on the basis of privilege. In that type of situation, the prosecutor reasonably expects to cause the disclosure of privileged information to the trial judge and would be well advised to file a s. 38.01 notice at an early stage in the proceedings. In other cases, the prosecutor might reasonably expect that the defence will ultimately bring an application to compel disclosure of withheld information at trial, but the defence appears to be refraining from serving a s. 38.01 notice in a timely manner. In those circumstances, the prosecutor might well consider serving the notice on the basis that the prosecutor expects to disclose the privileged information to the trial judge for review.

unconstitutional.[63] His ruling was eventually overturned by the Supreme Court of Canada,[64] but rather than wait until that appeal was decided (and occasion the risk associated with incurring delay in an important prosecution), the CSIS Director agreed to authorize disclosure[65] of the redacted materials to the trial judge for the purpose of determining whether they were protected by public interest immunity. The trial judge then embarked on a review of the redactions that were the subject of claims of national security privilege, "approximately 787 redactions in hundreds of documents."[66] The hearing conducted by Justice Dawson, a trial judge with deep experience in criminal law and criminal trials, took 15 days over roughly a month and a half, resulting in a comprehensive, written decision three days later.[67]

We were fortunate that we were able to conduct the section 38 review before Justice Dawson, and that he was able to dispose of the application so quickly. Had he not been able to carry out the review, it would have been conducted in the Federal Court and likely resulted in considerable delay. The bifurcation of the review of disclosure in the context of a criminal trial proceeding is exceedingly problematic from a prosecutor's perspective, as I discuss below.

B. The Trouble with Bifurcation

The decision whether to order the disclosure of information that is subject to national security privilege requires a balancing of interests. On the one side of the scale is the degree of harm that would be occasioned to national security through disclosure; on the other side is the impact that non-disclosure would have on an accused's right to make full answer and defence. These are both exceedingly important interests in the abstract, and where the balance is struck will very much depend on the nature of the classified information and the extent to which that information may assist in the determination of triable issues.

The rationale for vesting the jurisdiction to determine questions around national security privilege in the Federal Court seems to have been

---

63 R v. Ahmad, [2009] O.J. No. 6161.

64 R v. Ahmad, 2011 SCC 6.

65 Pursuant to s. 38.01(6)(c) of the *Canada Evidence Act*.

66 R v. Ahmad, [2009] O.J. No. 6156 at para 1 [*Ahmad* 6156].

67 The time taken to conduct the review by Justice Dawson was much quicker than the time it typically takes to complete a s. 38 review in the Federal Court.

two-fold: (1) the Court has expertise in relation to national security matters, flowing from the fact that it is the Court that issues warrants under section 21 of the *Canadian Security Intelligence Act* and (2) the Court has both the physical facilities and security-cleared personnel to manage classified material. These are not insignificant considerations, but when held up to scrutiny, they do not adequately justify the bifurcation of disclosure proceedings.

Superior court trial judges should have little difficulty grasping the nature and importance of national security interests.[68] The assessment of whether an intelligence agency's sensitive information should be disclosed is not much different from the assessment of whether a police agency's sensitive information should be disclosed, and the considerations that must be taken into account are often quite similar. Intelligence agencies and the police are both concerned about disclosures of sensitive investigative techniques; they are both concerned about compromising the identities of their human sources; and they are equally concerned about disclosing caveated information that they have obtained from third-party (typically foreign) agencies. The concern that disclosure of seemingly innocuous details and information, when read together, could identify a source – the so-called "mosaic effect" – arises regardless of whether one is talking about a CSIS confidential human source or an RCMP police informer.[69] The nature of the national security interests at stake, and the harms to those interests that would be caused through disclosure, are established in section 38 hearings through oral or affidavit evidence tendered by the Crown. There is little reason to think that superior court judges would be any less likely than Federal Court judges to give due regard to the national security interests at stake in an application for disclosure.

Classified information can also be managed and protected in a secure manner in criminal trial courts. Indeed, the reality is that superior court judges are already dealing with classified information. Many of the affidavits submitted to superior court judges in support of applications to intercept communications in the context of terrorism-related investigations contain information classified as "Top Secret." CSIS records containing sensitive,

---

68 See for example, *Ahmad* 6156, O.J.

69 Criminal courts have made explicit reference to the mosaic effect in declining to order disclosure of information relating to a police informer. See, for example, R v. McKay, 2016 BCCA 391 at paras 20, 155; R v. Chui, 2018 ABQB 899 at para 28.

classified information have been reviewed by superior court judges conducting terrorism trials.[70] Although provincial courthouses typically do not meet the standards required to store sensitive, classified information, it should be possible to implement procedures on an *ad hoc* basis, responsive to the needs of the individual case, the same way that classified information is handled in the United States under their *Classified Information Procedures Act* (*CIPA*).[71]

U.S. federal district courts, which have trial jurisdiction in federal criminal proceedings, are frequently called on to review sensitive, classified information under *CIPA* to determine whether the information must be disclosed to a defendant. They are also often called upon to review the legality of *FISA* warrants issued by the Foreign Intelligence Surveillance Court under the *Foreign Intelligence Surveillance Act of 1978*.[72] While the Foreign Intelligence Surveillance Court has a secure facility, security arrangements that may be required in a District Court with respect to the handling and storage of classified information are addressed on a case-by-case basis.[73]

---

70 *Ahmad* 6156, O.J.; R v. Jaser, 2014 ONSC 6052; R v. Alizadeh, 2014 ONSC 1907. I was the lead prosecutor on the *Ahmad* and *Jaser* prosecutions and am aware that the trial judges reviewed classified information under special procedures that we developed in each case. My former colleague, Jason Wakely, prosecuted the *Alizadeh* matter and advised me that the trial judge in that case also reviewed classified information under special procedures put in place for that case.

71 18 U.S.C. App. III.

72 50 U.S.C. § 1801 *et seq*.

73 Davis S. Kris and J. Douglas Wilson, *National Security Investigations and Prosecutions*, 2nd ed. vol. 2 (Thomson Reuters West, 2012), 144; Bruce M. MacKay, "The Use of Classified Information in Terrorism Trials," *Southern Illinois University Law Journal* 42 (2017): 78. Under *CIPA*, the Chief Justice of the United States was required to issue security procedures to protect classified information. Those procedures call for the appointment of a classified information security officer, the storage of classified information in a safe and approved containers in secure areas that meet government standards for storing classified information, and that court personnel who will have access to the classified information hold appropriate security clearances. See *Revised Security Procedures Established Pursuant to Pub L 96–456, 94 Stat 2025 , by the Chief Justice of the United States for the Protection of Classified Information*, 18 U.S.C. App. 9. Similar procedures were implemented in the *R v. Ahmad* and *R v. Jaser* cases. In *Ahmad*, the classified information was stored on encrypted laptops that were kept in a secured facility when the trial judge was not reviewing the information. In *Jaser*, the classified information was contained in a binder that was kept in a locked briefcase and stored in a secure facility when it was not required for review by the trial judge. In each case, once

There is no real basis for the view that national security would be inadequately safeguarded in superior courts if those courts were to have the jurisdiction to determine section 38 applications. The nature of the national security interests at issue are similar to the public interest immunities that arise in complex criminal trials involving criminal organizations. Moreover, the superior courts already handle sensitive information and *ad hoc* measures can be put in place to protect classified information from unauthorized disclosure. In sum, superior courts are equally capable of assessing the national security part of the balancing that is required under section 38 and of protecting the information.

When we turn to the other side of the balance, the assessment of the impact of non-disclosure on the right to make full answer and defence, there is a distinct advantage to conferring jurisdiction on the superior courts to determine section 38 applications and to involving the prosecutor in the process.

Assessing the impact of non-disclosure requires a sound understanding of the nature of the criminal proceeding and the viable issues that are likely to arise at trial. Many of the issues that arise, such as *Garofoli* reviews of authorizations and warrants, can be complex, and evaluating the actual usefulness of information to the determination of those issues often calls for sophisticated expertise in criminal law, the type of expertise that is found in many superior court judges.

In addition, superior court trial judges who hear disclosure applications in the context of criminal trials benefit from submissions from both the prosecutor and the defence. A superior court judge, therefore, obtains the benefit of getting the perspective of the prosecutor – an individual who carries out a quasi-judicial role requiring objectivity, fairness, and independence – on the nature of the allegations, the anticipated evidence, the criminal law issues in play, and the utility of the information at issue to the determination of those issues.

In contrast, the Federal Court has no institutional expertise in criminal law or criminal trial proceedings. Moreover, the counsel who have carriage of section 38.06 hearings in Federal Court on behalf of the Attorney General of Canada are typically litigation counsel from the Department of

---

the materials were no longer required, the trial judges ordered that the materials be sealed and stored in a secure government facility. The process followed in R v. Alizadeh, 2013 ONSC 7540 was the same as in *Jaser*.

Justice who often have little to no background in criminal law or conducting criminal trials. If the court appoints *amicus* to assist the court, *amicus* may or may not have expertise in criminal law.

Although the accused person is invariably granted party status and given an opportunity to make submissions, the prosecutor is afforded no role in section 38.06 hearings and is often kept in the dark on the status of any application. Indeed, in the Toronto 18 case, the prosecutors only learned that Justice counsel had filed an application in the Federal Court when defence counsel advised the trial judge of the fact that they were participating in case management teleconferences convened by the Chief Justice of the Federal Court.

Thus, the section 38.06 hearing in the Federal Court is heard and conducted by actors who, except for defence counsel, come to the application with no knowledge of the underlying criminal trial proceeding and have little to no expertise in criminal law or the conduct of criminal litigation. The perspective of an important participant in the underlying criminal litigation – the prosecutor – is effectively muzzled. Pace and momentum, so important to the conduct of a criminal trial proceeding in the post-*Jordan* world,[74] are lost as an important issue is hived off for determination in a distant court. Neither the United Kingdom nor the United States proceed in this manner: the determination of whether the public interest in disclosure outweighs the public interest in non-disclosure is made by the judge overseeing the criminal trial; the applications are brought by the Crown Prosecution Service in the United Kingdom and by federal prosecutors in the United States. The section 38 regime is constitutional, but it leaves much to be desired.

IV. NAVIGATING NATIONAL SECURITY: DISCLOSING RELEVANT INFORMATION IN CSIS HOLDINGS

The defence in the Toronto 18 obtained extensive disclosure of the RCMP investigative file materials, but they wanted to reach beyond that and obtain production of all information that CSIS held relating to any of the accused persons. Their argument was that CSIS was an investigating agency

---

74 Under R v. Jordan, 2016 SCC 27, trials in superior courts should be completed within 30 months of the date that the charge was laid. Delay beyond 30 months will result in an infringement of the right to trial without unreasonable delay under the *Charter*, unless the delay is justified by exceptional circumstances or caused by the defence.

that investigated the accused in relation to terrorism, and, as such, CSIS was subject to the same corollary obligation as the police to provide the fruits of their investigation to the prosecutor.[75]

The trial judge rejected this argument, concluding that the corollary obligation only arose in relation to the "fruits of a police or similar investigation undertaken as the foundation for a particular prosecution."[76] As Justice Dawson recognized, although CSIS conducted a wide-ranging investigation of the accused and other persons, it did so in furtherance of its own intelligence mandate, not for the purpose of prosecution.

The presumption that the fruits of an investigation are likely relevant to the prosecution of the charge, which is the underlying rationale for the Crown's *Stinchcombe* disclosure obligation and the corollary duty placed on the police, is not applicable to an investigation conducted for a different purpose and kept separate from the police investigation. The mere fact that CSIS shared some limited information with the police did not impose an obligation on CSIS to disgorge all of their holdings relating to the accused to the prosecutor.[77]

The defence were, therefore, required to meet the *O'Connor* standard for the production of records that were held by CSIS. Under *O'Connor*, an applicant who seeks the production of records in possession of a third party must first establish that the records exist and are likely relevant to the determination of an issue at trial. While the burden to establish likely relevance is not onerous, bare assertions of relevance will not suffice. The applicant must show some basis to believe that the records sought will assist in the determination of a triable issue. If the applicant meets this threshold requirement, the records are produced to the judge, who then assesses their true relevance. But at this second step of the *O'Connor* test, the judge should only deny production of the records where it is apparent after inspection that the records are clearly irrelevant.

We had concluded relatively early on that the defence would be able to meet the threshold of showing likely relevance for certain records in the possession of CSIS. For example, Shaikh and Elsohemy were both expected to testify at trial about events that they had witnessed while they had been

---

75 R v. Ahmad, [2009] O.J. No. 6153 at para 5 [*Ahmad* 6153].

76 *Ahmad* 6153, O.J. at paras 18–19.

77 The same result was reached in R v. Alizadeh, 2013 ONSC 5417 at para 15; R v. Nuttall, 2015 BCSC 1125 at para 46; R v. Peshdary, 2017 ONSC 1225 at para 9.

CSIS sources. There was a reasonable basis to believe that records existed within CSIS that were contemporaneous to the events in question and recorded what Shaikh and Elsohemy had communicated to their source handlers and that those records were likely to be more useful than the source debriefing reports prepared by the police, which were created sometime after the events and deliberately omitted specific details to protect source identities.

At the time, CSIS did not maintain individual investigative files like the police do, but rather maintained the information it gathered during intelligence investigations in different source holdings, some electronic, some hard copy. I concluded that even if only a small subset of records in the CSIS holdings were likely relevant to a few discrete triable issues, combing the database for relevant records would be a laborious process. Although the Supreme Court had yet to articulate the Crown's *McNeil* duty,[78] there was little point in waiting for the inevitable *O'Connor* application to begin the search for records possessed by CSIS that were likely relevant. We, therefore, adopted a pro-active approach and asked the Service to search for records relating to certain areas of likely relevance that we defined for them.[79]

The process of reviewing and culling the CSIS holdings took many months. The Service first searched for records relating to the various accused. CSIS counsel and DOJ counsel then reviewed those records and identified approximately 600 records for review by the prosecutors. Two prosecutors then reviewed those documents, applying a generous approach that tended to be over-inclusive, and determined that 284 of them should be disclosed to defence, with redactions applied to protect national security

---

78 *R v. McNeil* was handed down approximately six months after we initiated the review process with CSIS.

79 The areas of likely relevance were defined by the Crown in consultation with the defence. They were the product of negotiation, meaning that they were broader than probably would have been ordered by a court. And one of the areas of relevance would be resisted by the Crown under the law as it has developed in the intervening years. In the Toronto 18, CSIS agreed to produce any information in its possession that pertained to grounds set out in the police authorizations and search warrant applications, including records that would undermine the grounds. See *Ahmad* 6153, O.J. at para 67. In World Bank v. Wallace, 2016 SCC 15, decided several years later, the Supreme Court clarified that records held by a third party will ordinarily not be relevant to the review of an authorization or search warrant, because that review is concerned with the affiant's belief in the grounds. *World Bank* is discussed in Part V below.

privilege.[80] The trial judge subsequently reviewed the redactions and upheld the vast majority of them.

As illustrated in the case of the Toronto 18, although it is wrong to presume that records outside of the police investigative file are relevant, records that are in the possession of CSIS, or any other government agency, may well still be relevant to a triable issue and subject to production under the *O'Connor* test. Whether they are likely relevant will depend on the nature of the issues arising in a particular prosecution and the extent to which the records could reasonably assist in the determination of those issues. Any concerns about disclosing information that could cause injury to national security can be addressed by redacting the information and asserting public interest immunity.

The potential need to search the holdings of an intelligence agency for relevant information is not unique to national security prosecutions in Canada. Depending on the circumstances of an individual case, prosecutors in the United Kingdom, United States, and Australia also may be obliged to make enquiries of members of the intelligence community in an effort to obtain information relevant to the defence. In the United States, for example, the Rule 16 discovery obligation applies to the "government" writ at large, not just the prosecutor. Thus, federal prosecutors there often have to make enquiries of other government agencies, including members of the intelligence community, in order to comply with Rule 16. The decision whether to search for information held by an intelligence agency is typically guided by the concept of "alignment" in the U.S. If there is sufficient alignment between the intelligence agency and the investigation, the prosecutor is required to determine whether the intelligence agency is likely in possession of discoverable material under Rule 16. The prosecutor does so by requesting the intelligence agency to search its holdings for records relating to specific issues. Once the agency has identified records for review, the prosecutor attends and determines whether the material is discoverable. If it is, the prosecutor may resort to the provisions of *CIPA* to withhold the information or disclose it in a fashion that will not compromise national security. This is not much different than how the disclosure process unfolded in the Toronto 18 case.

When CSIS shares information with police investigators during an investigation, it may result in CSIS being required to produce further

---

[80] *Ahmad* 6153, O.J. at paras 67–72; R v. Ahmad, [2009] O.J. No. 6166 at para 10.

information for the purposes of the trial. The scope of production is shaped by (1) the nature of the information shared and (2) the issues at trial. In some instances, it is easy to anticipate the breadth of production that will ensue from information sharing. For example, if a CSIS human source, like Shaikh, becomes a Crown witness testifying to events that were first recounted to the Service, it is reasonable to anticipate that notes made by the CSIS source handler and other records relating to the reliability and credibility of the source might readily meet the test for production under *O'Connor*. If a CSIS surveillance officer observes a significant event and is going to be a witness at trial, any notes made by the officer will need to be produced.

In other instances, it will be much more challenging to assess the extent to which information sharing by CSIS may lead to demands for the production of further information at trial. In particular, when the information provided by CSIS has been relied upon by the police to obtain authorization to intercept communications, what are the implications for the production of additional information from CSIS holdings? Can the defence obtain production of the CSIS facting documents[81] relating to that information? If the shared information was obtained under a section 21 warrant (of the *CSIS Act*), can the defence require production of the CSIS warrant, the CSIS affidavit, and even perhaps the records relied on by the affiant?

V. NAVIGATING NATIONAL SECURITY: THE *GAROFOLI* REVIEW

As described in Part II above, in the Toronto 18 investigation, the information provided by CSIS in Advisory Letters became part of the foundational grounds used by the police to obtain their first authorization to intercept communications. When additional CSIS records were produced in response to the defence's *O'Connor* application, it became clear that some of the grounds relied on by the police had been obtained as a consequence of CSIS intercepting communications under a section 21 warrant. This created a thorny issue for the prosecution because of the rule that requires a judge reviewing a warrant or authorization for compliance

81 A "facting document" is the document in CSIS holdings that was relied on by the affiant to assert a particular fact in the affidavit.

with section 8 of the *Charter* to excise from the supporting affidavit any grounds that were obtained in contravention of the *Charter*. Under this rule, if the CSIS warrant was constitutionally deficient, any communications intercepted under that warrant and relied on by the police as grounds in their affidavit would have to be excised on review. Some further explanation about the review process may help in understanding how this issue unfolded at trial, the challenge it posed for the Crown, and how we dealt with it.

Assuming the accused have standing,[82] they have a constitutional right to challenge the admissibility of evidence seized by the state. Where the evidence at issue is a communication intercepted under a wiretap authorization, the defence may bring what is commonly referred to as a *Garofoli* application and seek to challenge the reasonableness of the search under section 8 of the *Charter*. A *Garofoli* application involves an examination of the record that was before the issuing judge and the determination by the reviewing judge whether the statutory preconditions for a wiretap authorization were met.

The standard of review is narrow. The focus is on whether the affiant reasonably believed in the existence of grounds that were sufficient to satisfy the statutory preconditions.[83] Errors or misstatements in the affidavit must be excised by the reviewing judge, but only if the affiant knew or ought to have known of the error or misstatement.[84] In addition, if the error or misstatement is a minor or technical error that was made in good faith, it need not be excised – the reviewing judge can amplify the record to correct the mistake. Omissions of material facts that were known or ought to have been known by the affiant are addressed by adding those facts to the affidavit that was before the issuing justice. Once the record has been

---

82 R v. Edwards, [1996] 1 S.C.R. 128, [1996] 1 R.S.C. 128; R v. Marakah, 2017 SCC 59.

83 *World Bank*, SCC at paras 117, 119.

84 *World Bank*, SCC at para 121 ("the accuracy of the affidavit is tested against the affiant's reasonable belief"). The observant reader will have noted that we agreed to produce records in the hands of CSIS that related to the grounds set out in the police affidavit. Why did we do so, when those records were not in the hands of the affiant and thus could not inform his belief? The answer is that the law was somewhat unclear at the time. We thought it possible that the defence could argue that, because CSIS had reviewed the draft affidavit, factual errors that CSIS ought to have caught should be excised. The position of the Crown today would be quite different as a result of the decision in *World Bank* – generally speaking, the production of records in the hands of CSIS to establish errors or omissions in the RCMP affidavit would not be relevant to the *Garofoli* review. See *World Bank*, SCC at para 124.

amplified to take into account material errors and omissions, the reviewing judge then asks whether the issuing justice, based on the record as amplified on review, could have granted the authorization.[85] In other words, does the affidavit, as amplified, set out enough reliable information to satisfy the statutory preconditions for issuance?

Although the *Garofoli* application is supposed to be concerned with what the affiant reasonably believed at the time the authorization was granted, this is not always the case under the current law. In a trilogy of cases[86] decided in the early days of the *Charter*, the Supreme Court held that information obtained as a result of a *Charter* violation must be excised from the supporting affidavit.[87] The rationale for this rule of automatic excision was that the state ought not to benefit from "the illegal acts of police officers."[88] Courts reviewing warrants and authorizations in a *Garofoli* application now routinely excise information obtained as a result of a *Charter* infringement, without asking the question of whether the affiant reasonably believed that the information had been gathered lawfully.

This rule of automatic excision is conceptually unsound and problematic for several reasons. First, under subsection 24(2) of the *Charter*, evidence that was obtained in a manner that infringed the *Charter* may only be excluded if its admission would bring the administration of justice into disrepute. The same evidence that must automatically be excised on a *Garofoli* review can nevertheless be admitted to determine guilt or innocence. In principle, it is difficult to understand why the state can use constitutionally deficient information to deprive a person of their liberty interest, perhaps for life, but cannot use the same information to deprive them of their privacy interest.

Second, a *Garofoli* application is concerned with the review of the evidentiary record – the sworn affidavit – that was before the issuing justice. The so-called "excision" of sworn evidence from that record on the basis of

---

85 R v. Garofoli, [1990] 2 S.C.R. 1421 at 1451–453, [1990] 2 R.C.S. 1421.

86 R v. Grant, 2009 SCC 32; R v. Plant, [1993] 3 S.C.R. 281, [1993] 8 W.W.R. 287; R v. Wiley, [1993] 3 S.C.R. 263, 84 C.C.C. (3d) 161.

87 The standing requirement applies at the excision stage. To seek excision of a fact as unconstitutionally obtained, the accused must show it violated his own *Charter* rights. He is not entitled to seek excision of facts allegedly obtained in violation of the rights of third parties. See R v. Chang, 2003 CanLII 29135, 170 O.A.C. 37 (ON CA); R v. Vickerson, 2018 BCCA 39.

88 *Grant*, SCC.

a *Charter* infringement really amounts to nothing less than the exclusion of evidence in the review proceeding. The rule of automatic excision is an automatic exclusionary rule that is contrary to the express wording of subsection 24(2) of the *Charter*.

Third, if the *Garofoli* application is supposed to be concerned with what the affiant reasonably believed at the time that the authorization was granted, it is confounding that the affiant's belief in the lawfulness of the grounds is not a relevant consideration.

Fourth, the rule of automatic excision is unnecessary to guard against unconstitutional acts of state agents. Under existing jurisprudence, evidence is obtained in a manner that infringed the *Charter* if there is a sufficient temporal, contextual, or causal nexus between the evidence and a *Charter* breach.[89] There is no need for a rule that magnifies the constitutional infringement and distorts the analysis under subsection 24(2) by taking the focus from where it should properly lie – on the initial breach and whether it warrants the exclusion of the evidence subsequently seized.

Finally, the rule of automatic excision has the potential to turn the *Garofoli* application into an expansive inquiry into collateral matters reaching far beyond the confines of the police investigation, generating time-consuming and sweeping disclosure requests. This was a real concern in the Toronto 18 prosecution.

The reader will recall that some of the grounds relied on by the police affiant in the Toronto 18 investigation came from the interception of communications by CSIS, acting under a section 21 warrant. The defence, therefore, contended that they should have access to the CSIS warrant and underlying affidavit, so they could challenge the lawfulness of the CSIS seizure of communications and argue for their excision from the police affidavit. But if the CSIS warrant, in turn, rested on information intercepted under an earlier warrant, then that warrant and its supporting affidavit would need to be produced, and so on, and so on.[90] We expected that the defence would also argue that, in order to challenge the CSIS

---

89 R v. Goldhart, [1996] 2 S.C.R. 463, 136 D.L.R. (4th) 502; R v. Strachan, [1988] 2 S.C.R. 980, 56 D.L.R. (4th) 673.

90 At one point during discussions in open court, the trial judge said this reminded him of Russian nesting dolls that can potentially go on endlessly, and there had to be some point at which you stop. The retort of defence counsel might be that you stop when there are no more dolls to open.

warrant(s), they would need access to the source documents that were relied on by the CSIS affiant(s). Any CSIS materials ordered and produced would inevitably need to be heavily redacted to protect national security, and, depending on the extent to which judicial summaries could be prepared, it might not even be possible to conduct a review of a heavily redacted CSIS affidavit.[91] The CSIS investigation had been a broad, wide-ranging investigation extending over a significant period of time. There was a significant risk that the prosecution would be derailed by expansive disclosure requests to facilitate fact-checking by the defence. In order to avoid going down this road, the Crown decided not to rely on any of the information derived from the CSIS intercepts and agreed to the excision of that information on the *Garofoli* review. Once we made that decision, the CSIS warrant and affidavit were no longer relevant to a triable issue and thus not subject to production under the *O'Connor* framework.

This approach only worked in the Toronto 18 prosecution because there was enough information remaining in the police affidavit after excision to support its issuance. Many of the grounds had been furnished by Shaikh, and those grounds had been substantially corroborated by observations made by both the police and CSIS. In cases where the police authorization rests on CSIS interceptions, a similar approach would be fatal to the police wiretap. However, the law relating to production from third parties in the context of a *Garofoli* application has been developed and clarified since the Toronto 18 case. Where a third-party agency seized evidence under judicial authorization and that evidence was relied on as grounds to obtain a wiretap by a police affiant, there are solid arguments that can be advanced supporting a narrow scope of production from the third-party agency and keeping the *Garofoli* application within reasonable bounds.

In light of *World Bank* and its reminder that the *Garofoli* review is focused on the affiant's reasonable belief, it seems to me that the question that should actually be asked on the review is not whether the grounds relied

---

[91] Under the *Garofoli* "Step Six" procedure, a judge reviewing a redacted affidavit may consider the redacted material in assessing the sufficiency of the warrant, but only if the defence have been provided with a judicial summary of the nature of the material that is sufficient to permit them to challenge it by way of evidence or submissions. Moreover, the Step Six procedure was not being used by criminal courts at the time of the Toronto 18 prosecution. It was not until the later decisions in *R v. Learning*, 2010 ONSC 3816, and *R v. Rocha*, 2012 ONCA 707, that the Step Six procedure was resurrected.

on by the affiant were legally obtained, but rather whether the affiant reasonably believed that the grounds had been legally obtained. The focus should be on whether the affiant knew, or ought to have known, that the grounds were the product of an unlawful seizure. If the affiant reasonably believed that the grounds were legally obtained, there is no basis upon which to excise that information from the affidavit. I appreciate that this calls for an end to the rule of automatic excision, but it is a rule that is suspect and should be discarded.[92]

As I pointed out above, abandoning the rule of automatic excision would not mean that prior state illegality would be insulated from review in all instances. If the accused can establish that there is a sufficient nexus between the gathering of the evidence and previous state illegality, then the accused can still seek exclusion of the evidence under subsection 24(2).

But discarding the rule would have the benefit of keeping the production of material from third parties in the context of *Garofoli* applications within reasonable bounds and maintaining consistency of approach in the review of the affiant's belief. In the Toronto 18 prosecution, if what mattered was the affiant's reasonable belief in the lawfulness of the CSIS information, there would have been no basis for production of the CSIS warrant, affidavit, or source documents. Unless the defence could point to some evidence to the contrary, the affiant was entitled to reasonably believe that CSIS had acted lawfully under its mandate.

If it is thought to be too radical of a step to get rid of automatic excision, it may still be possible to keep production of CSIS records within reasonable bounds by insisting on a strict application of the principles articulated in *World Bank* and *O'Connor*. That is, the disclosure of third-party records should only be ordered where the accused shows that the records will tend to undermine one of the statutory preconditions for issuance of the police authorization. This might justify production of the CSIS warrant and the underlying affidavit in a redacted form to the defence because those documents are probative of whether the CSIS warrant was lawfully issued.[93]

---

92 Ireland has an almost absolute exclusionary rule where evidence was obtained in conscious and deliberate violation of constitutional rights, and a presumptive exclusionary rule where the constitutional violation was not conscious and deliberate. See Director of Public Prosecutions v. JC, [2015] IESC 31 (SC Ireland). However, unconstitutionally obtained evidence may be relied on to obtain a warrant. See *JC*, IESC at para 65; Director of Public Prosecutions v. Cash, [2010] IESC 1 (SC Ireland).

93 *Alizadeh*, ONSC.

But without more, it would not justify production of source documents relied on by the CSIS affiant or previous CSIS warrants and affidavits – extending the scope of production this far begins to look like a fishing expedition and inefficient use of resources. Absent some basis for believing that the CSIS affidavit contains misstatements or material omissions, production of the source documents relied on by the CSIS affiant should be refused.[94]

So far, I have discussed the scope of production from CSIS in the context of a *Garofoli* review of the police wiretap authorization, assuming that we continue to retain the rule of automatic excision. But what if the defence wishes to bring a *Strachan*-type of argument and seek the excision of communications intercepted by the police on the basis that there is a sufficient temporal, contextual, or causal nexus to a CSIS warrant that allegedly infringed the *Charter*? Here, again, I would argue that the answer lies in *World Bank* and *O'Connor*. If the defence can show that a sufficient nexus exists, there is a basis upon which they can seek production of the CSIS warrant and affidavit. Those documents are likely relevant to the determination of the legality of the CSIS warrant, and the legality of that warrant is determinative of the admissibility of the evidence seized by the police. Going beyond those documents into underlying CSIS source documents is not justified – the only reason to obtain production of the latter is so the defence can engage in "fact-checking." Absent some basis for believing that the production of source documents will tend to undermine facts set out in the CSIS affidavit, production should be refused.[95]

---

94 *Alizadeh*, ONSC.

95 The same approach should be followed if the Crown seeks to tender into evidence a communication intercepted by CSIS. While the defence has a right to challenge the admissibility of that evidence and, therefore, a right to disclosure of the CSIS warrant and supporting affidavit, absent some reasonable basis for believing that source documents will undermine the grounds set out in the affidavit, disclosure of source documents should generally be refused. The mere assertion that the records might assist in "fact-checking" of statements in the affidavit is not a sufficient basis to require the production of source records from a third-party agency. See, for example, R v. Grant, 2013 ONSC 7323, where the accused sought to subpoena a confidential informant's file (a third-party record) so that the judge could then compare the way the CI was described in the Information To Obtain (ITO) with the facts reported in the CI file. Justice Goldstein refused to order production, holding that if the accused has not shown a reasonable likelihood that the file contained information that would undermine the ITO, then there was no basis to order its production simply to engage in comparative fact-checking. He described this as "random virtue testing" of the affiant.

VI. Conclusion

Effective investigations of terrorist groups will often require that the police and intelligence agencies share intelligence information. When the police rely on sensitive information relating to national security in the course of their investigation, complex issues will almost inevitably arise for the prosecutor. However, as I hope this chapter demonstrates, experience to date has shown that the challenges that arise can be managed in a principled manner without compromising either national security or the accused's right to make full answer and defence.