PROFESSIONAL DEVELOPMENT INSTITUTE

INTELLIGENCE AS EVIDENCE

BRIEFING NOTE

Authors: Gérard Normand, Alan Jones

uOttawa

Institut de développement professionnel
Professional Development Institute

Introduction

The expression "*intelligence as evidence*," or turning intelligence into evidence, has been at the centre of a longstanding issue in Canadian national security law. This note will address misconceptions surrounding it. The note will provide an explanation as to the nature of these two separate notions, intelligence and evidence. It will analyze the nature and methods relating to both intelligence and criminal investigations, the intended use of these two types of information and how they conceptually differ in the context of a prosecution. It will finally detail the complex process to be followed, as well as the assessment to be undertaken, both by CSIS and a prosecutor before even considering using intelligence as evidence in the context of a criminal trial.

Of note, this note will deal with intelligence as evidence specifically in a criminal law litigation context. However, the basic principles found in this note would be equally applicable to other types of litigation, albeit with different rules with respect to the admissibility of evidence.

Background

Canada, like many other democratic countries, has legislation enabling particular agencies to either conduct investigations to produce intelligence that provides insights and often forewarning on threats to the security of Canada, or conduct investigations in order to gather evidence to prosecute those who commit criminal offences, including terrorism or security-related offences that may undermine its national security. These two types of mandates are quite different and are not interchangeable.

In addition, Canada adopted the *Constitution Act,* 1982, part of which is a *Charter of Rights and Freedoms*, and enjoys a long common law tradition that applies in all matters of public law, such as criminal law. These authorities provide for the foundational basis that has helped to shape the rules governing the collection and handling of evidence as well as to define individuals' right to challenge the evidence presented against them in a criminal court of law.

Evidence is gathered by the police and intended to be used publicly in a prosecution before a court of law. Evidence must be collected and handled on the basis of specific rules in order to make admissible and therefore usable against an accused. Intelligence is not gathered under evidentiary rules because it is collected for a totally different purpose, one of advising and reporting to the government on threats to the security of Canada.

Terrorism-related activities covered by the *CSIS Act* must meet the definition of a threat to the security of Canada. These same activities may also contain the elements of potential criminal offences. In such cases, there exists a possibility of having an overlap of investigations between CSIS and RCMP. The question that sometimes arises is why intelligence gathered through CSIS investigations cannot simply be provided to the RCMP for use as criminal evidence in a prosecution. The answer to that question is far from simple, and has *Charter* as well as legal and operational implications.

The public's understanding of the notion of intelligence as evidence has been shaped by the media, which in turn often comes from academic commentary on national security issues. It is not uncommon and perhaps not surprising that the media or academia all too frequently misunderstand the law around this complex issue and portray it as simply stemming from bureaucratic intransigence or "turf wars" that could easily be resolved by everyone being a team player.

Controversy around this issue is usually associated to scenarios where agencies, often CSIS, are allegedly holding onto and refusing to provide intelligence that could be used as valuable evidence in a national security prosecution. These scenarios are based on a mistaken characterization of the legal nature of intelligence versus evidence. As a result, there are sometimes calls for the federal government of the day to adopt legislation directing that intelligence, from whatever organization producing it, could or should be used directly as evidence in a court process.

This note will break down and explain the law underpinning the notions of intelligence and evidence, and provide a rationale as to why there are no "quick fixes" possible to the issue of using intelligence as evidence.

The Law

The two concepts of intelligence and evidence are of paramount importance to the government in the national security realm. They are aimed at protecting the country, at ensuring the safety of its citizens and the proper functioning of society. However, they are grounded on two totally different legal basis.

Indeed, their collection, use and sharing fall under two regimes that are guided by different laws and authorities, and based on different mandates.

A) Criminal versus Intelligence investigations

Before delving specifically into the rules of admissibility of evidence, and the impact it will have where intelligence is being considered to be used as evidence, we will analyze some general principles applying to each type of investigation that are based on very different and separate mandates.

Information – Purpose of collection

Information collected through a police investigation serves as the basis to arrest, charge and prosecute an individual with respect to a criminal offence. This information will become evidence if it is determined to meet strict rules of admissibility before a court of law in the context of a public prosecution. As a constitutional principle, all evidence, save exceptions, must be disclosed to the accused.

In Canada, criminal offences, including crimes related to national security, are essentially found in the *Criminal Code*. The police are legally entitled to make use of their powers, including conducting a search or using a wiretap, to gather evidence in the context of an investigation of an individual who is believed to have committed a criminal offence. The police cannot base their criminal investigation under the CSIS Act.

CSIS conducts investigations relating to activities that may on reasonable grounds be suspected of constituting a threat to the security of Canada as defined by the *CSIS Act*. CSIS does not investigate under the *Criminal Code*. It

produces, for the purposes of this note, what is referred to as "intelligence". Some activities constituting a threat to the security of Canada under the *CSIS Act* may also become criminal offences.

Intelligence serves to advise and report to the government. In some cases, it can be a forewarning to police that a serious crime such as terrorism or espionage offence might be developing. That being said, most pieces of information used to create a CSIS intelligence assessment would rarely be viewed as "accurate enough" or "verifiable enough" to ever be considered criminal evidence, but they still remain very useful pieces of an information puzzle about a potential threat. Intelligence is often an incomplete picture that precedes the police identifying elements of a criminal offence. This is largely because intelligence is not/never collected to satisfy the rules of criminal evidence. If activities justify a criminal investigation, it must be, along with the collection of evidence, undertaken by the police.

If information gathered by CSIS for intelligence purposes would have to be gathered in accordance with the strict rules governing the collection of admissible evidence, the ability to forewarn would be exceptionally rare, if ever take place at all.

Nature of collection methods

Although the collection methods between the two types of investigations are similar in many ways, peace officers will generally perform their collection activities overtly. More importantly, the results of their investigative methods are, save exceptions, exposed publicly in the context of a prosecution.[1]

CSIS Intelligence officers perform much of their collection activities covertly. The sensitive nature, methodology and intelligence resulting from CSIS investigations necessitate the long-term protection of those details from public exposure. This is basically because they would otherwise end up, by extension, known by the subjects of national security intelligence investigations, thereby causing injury to national security.

At the international level, Canadian police forces may receive and use, in the context of a Canadian prosecution, evidence gathered abroad by foreign police forces but only if the evidence is determined to be admissible under Canadian law.

Allied foreign intelligence agencies often operate under a similar regime as in Canada. They regularly share threat-related intelligence with Canadian agencies such as CSIS. Sharing arrangements involving CSIS is based on the principle that shared intelligence remains the property of the originator and that without an express written consent, it may not be further disclosed or used by the recipient agency. This is known as a *caveat*. This alone would prevent the use of intelligence received from a foreign partner as evidence in a Canadian criminal prosecution.

Use and Lifetime of Information

Information collected by peace officers through a police investigation is meant to be used as evidence in the context of a prosecution. Once the proceedings are over and a judgment is rendered by a court, the lifetime of the evidence normally ends.

Intelligence collected by intelligence officers is to be statutorily used to report to and advise the government. Investigations are ongoing and may last for decades. There is no specific lifetime for this intelligence.

Public Versus Non-public Nature

Information collected by peace officers to be used as evidence may be publicly challenged by the accused before and at the trial stage, including on the basis that it does not meet the rules of admissibility of evidence or infringes the *Charter* rights and freedoms of the accused. Prosecution must be public by nature and there are very few exceptions to this rule. In addition, the accused has the right to be present at every step of his/her proceedings, and to see and hear all of the evidence.

The open court principle is one of the hallmarks of a democratic society, fostering public confidence in the integrity of the court system and the understanding of the administration of justice. The public disclosure of evidence is the norm.

At the other end of the scale, information collected by intelligence officers is not meant to be exposed publicly at all, i.e., non-public disclosure is the norm. Only persons with appropriate security clearances and a "need to know" can access it. In fact, statutory measures are in place to prohibit the public disclosure of intelligence in proceedings where injury to national security would result. In addition, specific offences relating to its non-authorized disclosure exists. Finally, in camera review mechanisms under both the *National Security and Intelligence Review Agency Act* and the *National Security and Intelligence Committee of Parliamentarian Act* are in place essentially in lieu of the fact that the public accountability of the activities of security agencies such as CSIS cannot take place.

B) Admissibility of evidence

As mentioned above, in order to be admissible as evidence, any information, and this would include intelligence, must abide by specific rules.

There are several types of evidence in criminal matters. The most frequent are testimonial, written, technical evidence (search and wiretapping), and evidence based on extrajudicial statements.

Testimonial evidence must be based on what a witness saw or heard, and/or on his/her personal knowledge of the facts. The witness must present his/her evidence in person before the court, in the presence of the accused and will be subjected to cross-examination.

Written evidence, as in a document or a report, can only be adduced and filed as evidence through a witness, save exceptions. The witness will need to be able to testify as to his/her personal knowledge of its content and the circumstances surrounding its writing. Generally speaking, the witness will need to have been the author of the document, or report, based on his/her own personal knowledge or experience, otherwise the document will not be admissible as evidence based on the hearsay rules. If outside sources were used to prepare the report (e.g.,

referring to intercepted communications), this would also constitute hearsay and would not be admissible as evidence, unless these other sources are established separately according to the rules of admissibility of evidence.

Extrajudicial statements are generally those of the accused, and their filing in evidence must be preceded by a *voir-dire* in open court so that the judge can be satisfied with the free and voluntary nature of the written statements. Extrajudicial witness statements cannot be entered into evidence. In order for their information to be declared admissible, witnesses must appear in court to testify in person and be cross-examined by the accused.

Evidence of a technical nature (search and seizures, production orders, wiretaps) must be preceded by a judicial authorization issued by a judge under the *Criminal Code* and these authorizations are reviewable by the trial judge if the request is made by the accused. The review takes place in open court and involves all the material that was before the authorization judge (including the affidavit of the applicant) in the initial *ex parte* application. The affiant may be publicly examined with the Court's permission on any aspect of the affidavit or other supporting information, and be cross-examined by the accused.

The source, the origin and the credibility of any information to be adduced as evidence must be publicly established to the satisfaction of the court. Otherwise, it will not constitute admissible evidence.

Intelligence

The *CSIS Act* enables the Service to collect, to the extent strictly necessary, analyze, and retain information and intelligence, in order to report and advise the government on activities related to a threat to the security of Canada.

The notion of "reporting and advising" carries some uncertainty about what exactly the government could/should "do" with that intelligence.

The intelligence enables the government to deal with its domestic security through various means. Intelligence can be used for some specific administrative purposes (citizenship, security clearance, issuance of license or permit) or for immigration control (inadmissible classes of persons, security certificates). Some of these processes, like in the *Immigration and Refugee Protection Act* (Division 9), have their own statutory internal regime to deal with intelligence in an *in camera* fashion (e.g., security certificates). In all other cases, using intelligence will almost always be at the cost of dealing with serious admissibility issues versus protecting the information from public disclosure.

Any intelligence shared by or to CSIS is always with a clear caveat, namely that the information provided will not be further shared or used without the knowledge and written approval of the originator.

The *Canada Evidence Act* contains provisions that explicitly prohibit sensitive or potentially injurious information from being released publicly in the context of proceedings where disclosure would cause injury to Canada's international relations, national security and/or defence.

The *Access to Information Act* contains similar provisions to prohibit the public release of intelligence whose public disclosure may be injurious to national security when an access request is made by any person. In addition, criminal offences have been created to protect the unauthorized communications of intelligence in the *Security of Information Act*.

All this supports the principle that intelligence is meant to remain outside of the public realm as disclosing it could ultimately be injurious to our national security.

Above all, the basic foundational principle underlying the collection of intelligence is that it is never done for the purpose of being used as evidence.

Collection Methods

In many ways, the methods of collecting intelligence are similar to the ones used by law enforcement, except that they are never meant to become known or exposed publicly in the former case. For instance, the use of human sources, of judicial warrants aimed at the interception of communications or at searches, or of physical surveillance units is present under both types of collection of information activities.

If there is one distinction, CSIS also regularly receives reports from allied foreign agencies. As such, these reports usually do not contain any indications of the source, of the origin of the intelligence forming part of them.

C) Use of intelligence as evidence

Based on the rules governing the admissibility of evidence discussed above, reconciling intelligence with admissible evidence would not appear, at first blush, to be an easy task.

Canada Evidence Act

But before getting into the specifics of this issue, it is important to highlight the provisions appearing at subsections 38.06(4) and (5) of the *Canada Evidence Act* (CEA).

Created in the context of the *Anti-Terrorism Act* in 2001 (through amendments to the CEA), they enable a judge of the Federal Court to authorize the introduction of some information as evidence (or a summary of it) if:

1. the judge finds that the disclosure of this information would be injurious if disclosed publicly, but
2. the judge nevertheless believes that the public interest in disclosing this information outweighs in importance the public interest in not disclosing it, and
3. the judge, after having considered all the factors that would be relevant for a determination of admissibility of evidence, orders the introduction into evidence in the main proceeding of the information, subject to any conditions fixed by that judge.

The Court must assess the intelligence based on the rules of admissibility of evidence.

The scheme provides that all this takes place *in camera* and *ex parte*, although nothing would prevent the Court from seeking the views of, for instance, an accused through his/her counsel. But neither the accused nor his/her counsel would be allowed to see the injurious information or challenge the admissibility of the information as evidence, *per se*.

However, the trial judge (the judge of the main proceeding) could, in the face of such intelligence permitted to be used as evidence, make any order pursuant to section 38.14 that he or she considers appropriate in the circumstances to protect the right of the accused to a fair trial, including by dismissing specified counts of the indictment or information, or affecting a stay of the proceedings. This would usually be because the accused would not have participated to the process. In addition, the trial judge could simply decide not to afford any legal weight to this evidence assessed by another judge and in the absence of the accused.

Analysis

Under this section, we will shed some light on what would practically and legally have to take place in order for intelligence to be considered to be evidence.

Human sources

As is the case in criminal matters, "informants" in the intelligence world rarely testify. The identity of intelligence sources must remain permanently protected. These sources may have taken years to develop, and often live in parts of the world beyond any possible witness protection program. They are often irreplaceable and, if exposed, would not only represent a loss of high value intelligence but they, and their families, may suffer major retribution, including death. Paramount to that, and in order to ensure the possibility of attracting such sources in the future, agencies like CSIS must respect their engagement that sources agree to co-operate on the condition that their identities will never be exposed in court.

The informant's privilege is probably the one, along with that of Cabinet confidences, most firmly anchored in Canadian law. A judge must even raise it *ex officio*. This is ultimately aimed at protecting the informant, i.e., the human source, from testifying. The only exception is where the information in the possession of the informant would go to the innocence of the accused, i.e., the innocence at stake exception. All this to say that intelligence obtained through a human source could not be considered to be used as evidence unless the source would agree to appear in person before the court and the accused to testify. And the risk of having injurious information disclosed by the source through his/her testimony or cross-examination would be very high.

Judicial Authorization/Warrants Issued by the Federal Court

Intelligence obtained as a result of a judicial authorization can, in theory, be used as evidence, but this would necessarily mean that a public open court review of the Federal Court's authorization pursuant to section 21 of the CSIS Act would have to take place. The affiant would be required to appear in person and testify in this open court process based on his/her affidavit that was provided to the Federal Court judge to have the warrant issued initially, and be cross-examined by the accused. In addition, any factual allegation appearing in the affidavit would be scrutinized. If one such allegation was based on a past intercept or a foreign agency report, then this could need to be unpacked as well in order to determine whether the resulting factual allegation was obtained in accordance with the rules of admissible evidence in Canada. We can easily imagine how difficult and damaging such a scenario would be for a security agency like CSIS to find itself in where its information is, as a rule, never discussed publicly.

Therefore, as a general rule, this type of involvement will rarely happen, for obvious reasons. But if the Service was to agree to take this route, it would need to face a number of difficult steps. First, CSIS would want, in the course of the review, to block as much information as possible in the affidavit, for security purposes. However, a sufficient amount of information would need to ultimately remain in the affidavit to establish the merits of the initial authorization.[2] Indeed, trying to demonstrate the validity of a judicial authorization by redacting too much

information would mean that the authorization would ultimately be quashed by the trial judge. As explained in footnote 2, the revised text must justify the authorization. If not, this could have the effect (see first part of para 6 in footnote 2) of preventing the prosecution from using the resulting intelligence obtained through the authorization. The attempt to have this intelligence determined to be admissible evidence would have failed. Not to mention that this review process would have publicly exposed a lot of CSIS information for no reason.

In conclusion, all of the above would need to be assessed and weighed by both CSIS and the prosecution before any charges are laid.

Foreign agency information

Turning to intelligence received from foreign partners, it must be understood that these reports normally do not identify their sources of intelligence, i.e., where the intelligence actually originates from. In fact, a foreign intelligence report could be a mixture of, for instance, a technical source, an interview from a community member as well as another foreign intelligence report. CSIS, for example, would never know the identity of a human source or the nature of a technical source unless the foreign agency agrees to provide this information.

In order for a foreign agency report to be admitted as evidence, officials of the foreign agency would have to appear in court and establish how their intelligence was obtained. Most importantly, it would also need to be established that this meets our Canadian criminal law's rules of admissibility of evidence. In addition, in order to be used as evidence, it would need to be established that using the foreign information against the accused would not infringe the rights and freedoms guaranteed by the Canadian *Charter*. Finally, foreign officials or citizens are not compellable to Canadian courts. They would have to agree to participate in such a process. There are historically very rare instances of such cooperation. CSIS once agreed to provide its information to be used as evidence, along with some witnesses, in an American prosecution of a terrorist.

Situation in Other Countries

The situation described in this note, with respect to criminal law proceedings, is essentially the same that take place in other countries of the G-7, as well as anywhere where the rule of law prevails. There are rules governing the admissibility of evidence in these countries as well. In order to use intelligence as evidence, the intelligence would need to follow a similar process as would any information to be used as evidence. The situation in Canada is not unique.

In the United Kingdom, the *Justice and Security Act 2013* introduced a Closed Material Proceedings procedure for civil litigation. This is a procedure whereby all or part of a civil claim can be heard in a closed proceeding presided the same judge that presides the public portion of the proceedings. The closed portion enables the judge to hear and consider evidence which, if disclosed publicly, would risk harming national security. The existence of this process does not relieve the government from establishing the admissibility of the evidence in the closed proceeding of the civil trial. However, these hearings exclude the other party, who is represented by a Special Advocate (there is no contact with the client, however, once the proceedings start). A summary of the non-publicly disclosed evidence is prepared by the judge, with the help of the government counsel and the Special Advocate, to be provided to the other party and argued in the public portion of the proceedings. This process is not applicable in criminal cases in the United Kingdom because the accused must be present throughout the proceedings, like in Canada.

In Canada, a Closed Material Proceedings process does not exist. However, Parliament could pass a similar legislation to that in the United Kingdom for civil and administrative litigation.

CONCLUSION

In order to contemplate using intelligence as evidence in the context of a criminal law proceeding, strict rules of admissibility must be considered. These are the same rules that must apply to any other type of information wanting to be used as evidence. The fact that it is intelligence does not make the rules any easier, simpler or different. Intelligence cannot automatically be made admissible under the rules of evidence. Therefore, a legislation that would require an intelligence agency to provide its intelligence that some are quick to label as "evidence," to the police is not only unthinkable in a democratic society but would not, could not legally represent a solution. Our criminal law regime must abide by its constitutionally based rules.

There is also one important inescapable consequence with respect to using intelligence as evidence: it would tend to publicly reveal a particular security intelligence investigation, the methods of collection employed and the nature and quality of its intelligence, all of which would cause, if disclosed publicly, injury to our national security.

Any intelligence, as well as the overall context of its collection, should be, at the time of the laying of criminal charges, closely and diligently analyzed by CSIS and the prosecutor keeping in mind the strict rules of admissibility if it is intended to be considered evidence, as well as the operational consequences. Otherwise, it could quickly become a "poison pill" for a prosecution. This is why CSIS and prosecutors will often choose not to entertain the idea of using intelligence as evidence.

Footnotes

[1] An example of the overt nature of criminal investigations appears in subsection 196(1) of the *Criminal Code* which requires the AG to provide notice to those whose conversations will have been intercepted through a wiretap warrant 90 days after the issuance of the warrant.

[2] In R. v. Garofoli (1990) 2S.C.R. 1421, the Supreme Court of Canada stated:
Dickson J. concluded that since the trial judge must verify the merits of the authorization, it will be necessary in most cases to open the sealed package. ... He concluded that the trial judge could not properly decide whether the interceptions had been made lawfully without examining the contents of the packets. Dickson J. also concluded that, on the basis of a substantive review of authorization, the accused must be given an opportunity to cross-examine the deponent. The questioning must focus on whether authorization was properly obtained, without disclosing the information that must be kept confidential.

And the Court then took the steps to follow:

1. When opening the package, if the Public Prosecutor's Office objects to the disclosure of any of the documents, it should, in a request, indicate the nature of the elements to be deleted and the reasons for doing so. Only the Crown prosecutor will have the affidavit at this stage.
2. The trial judge should then review the affidavit as proposed by the Crown prosecutor and provide a copy so prepared to counsel for the accused. The arguments of the accused's lawyer would then have to be heard. If the trial judge is of the opinion that counsel for the accused will not be able to assess the nature of the removed material based on the recommendations of the Crown prosecutor and the affidavit so produced, some sort of judicial summary as to the general nature of the deleted material should be provided.
3. After hearing the arguments of counsel for the accused and the response of the Crown, the trial judge should make a final decision on the revision of the documents, bearing in mind that it should be kept to a minimum and that the above factors should be applied.
4. Once the decision has been made according to step (3), the package parts should be returned to the accused.
5. If the Public Prosecutor's Office can justify the authorization on the basis of the revised documents, the authorization shall be confirmed.
6. However, if the revised text no longer justifies the authorization, the Crown may then request the trial judge to take into account the deleted elements to the extent necessary to justify the authorization. The trial judge should grant this request only if he is satisfied that the accused is sufficiently aware of the nature of the excluded evidence to challenge it in his or her closing arguments or in the evidence. In this regard, a judicial summary of the excluded evidence should be provided if it can fulfil this function. It goes without saying that if the Crown disagrees on the extent of the disclosure and believes that the public interest will be prejudiced, it may withdraw the evidence gathered through the wiretap.