This year’s questionnaire will explore the use in member countries of electronic devices as a criminal investigation tool to intercept communications. Technological advances have increased the sophistication of and the reliance by investigative agencies on devices to intercept all forms of communication transmission, from the use of microphones to capture face-to-face conversations, to wiretapping, to the interception of computerized and satellite communications.

This questionnaire will explore: (I) the conditions under which the electronic interception of private communications is authorized in member countries; and (ii) the legal principles that apply to the admissibility of evidence derived from the interception of communications.

This questionnaire does not address the electronic interception of private communications for the purpose of detecting terrorist activities as legislative responses of member countries to terrorist activities may be the basis for discussion at a future conference.

Topic I: The initial authorization to intercept private communications

1. (a) Does your country have special legislation that authorizes the interception of private communications to assist in the investigation of crime? X Yes □ No

If yes, does the interception require the prior authorization of a Court of law?

X Yes □ No

Yes, with one exception (see answer (b) below)

If yes, please answer questions (b), (c) and (d) below:

(b) what conditions must be present or criteria met before a Court will grant an order authorizing the interception of private communications?

The Criminal Code of Canada (“Criminal Code”) provides for several types of orders which allow the interception of private communications.

The most commonly granted order must meet the criteria set out in Section 186 of
the Criminal Code. A Court can only allow the interception where an offence listed in Section 183 of the Criminal Code (serious offence) is being investigated (ie. murder, robbery, theft, extortion, uttering threats, sexual assault). In granting a Section 186 order, the Court must be satisfied that:

1) there are reasonable grounds to believe that a serious crime has been or is being committed and that the interception of private communications will lead to evidence of this crime;
2) it would be in the best interests of the administration of justice to authorize the interceptions; and
3) the interception of private communications is necessary.

The interception of private communications is necessary only where other investigative procedures 1) have been tried and failed or ii) are unlikely to succeed or iii) the matter is so urgent that it would be impractical to carry out the investigation using other investigative procedures. The necessity requirement does not apply in the case of criminal organizations and terrorism offences.

The criteria for obtaining an authorization are less strict if one of the parties to the communication consents to the interception. Section 184 of the Criminal Code provides that where the originator or the recipient of the communications consents in writing to the interception, a Court may allow the interception of communication where there are reasonable and probable grounds to believe that any offence listed in the Criminal Code or any other federal statute has been or will be committed, and where there are reasonable and probable grounds to believe the interception will provide information concerning the offence. An application under Section 184 of the Criminal Code can by made by telephone, fax or email.

The Criminal Code also provides for granting orders authorizing the interception of private communication where:

- there is a risk of bodily harm to a party who consented to the authorization and the purpose of the interception is to prevent bodily harm (Section 184.1 of the Code);
- where the need for an order is so urgent that interception must be authorized before an order under Section 186 could be made (Section 188 of the Code). An order made pursuant to Section 188 can only last for 36 hours, and imposes limits on the interception to protect against excess;
- it is impractical for the applicant to appear personally before the authorizing judge. In such a case, the applicant can make the application by telephone or any other form of telecommunication (Section 184.3 of the Code). An authorization under this section can only last 36 hours.
Section 184.4 of the *Criminal Code* permits interception of private communications *without* prior Court authorization where:

1) the officer believes that the situation is so urgent that no authorization could be obtained under any other section of the *Criminal Code*;

2) the officer believes that the interception is immediately necessary to prevent an unlawful act that would seriously harm a person or property; and

3) either the originator of the recipient is the person who would cause the harm.

There is no case law dealing with this section of the *Criminal Code*, and some critics have suggested that the section may be unconstitutional.

© describe the hearing in which the application for an authorization to intercept private communications is granted. Who presents the application (police? prosecuting attorney)? How is the evidence presented (*viva voce*, by sworn written statement)? Is the application audio-recorded?

Either the police or the prosecuting attorney can present the application. Pursuant to Section 185 of the *Criminal Code*, except as indicated in answer (b) above, the application must be in writing and must be accompanied by a sworn written statement. The application must be signed by the Attorney General or the Minister of Public Safety and Emergency Preparedness, or an agent designated for that purpose by these Ministers. As the application is usually entirely in writing, it is not usually audio recorded. However, if there is an issue raised by the application that requires some oral communication between the judge and the applicant, it is prudent to audio record any oral exchange. This reflects the concern that the record should be complete in the event that the granting of the authorization is later reviewed.

(d) must the authorization to intercept private communications specify:

- what types of interception may be used (*ie.* microphone, interception of computer communications, wiretap of phones)?  **X Yes**  **□ No**

Section 186 of the *Criminal Code* provides that the authorization must generally describe the manner of interception that may be used. Section 186 has been strictly interpreted by the Courts, which have held that the order should make specific reference to the types of devices which may be used for the interception.

- the length of time the authorization remains in effect?  **X Yes**  **□ No**

Is there a maximum time provided by law that an authorization to intercept can remain in effect?  **X Yes**  **□ No**  If yes, what is that time?
Section 186(4)(e) of the *Criminal Code* provides that the authorization must state its duration, and that the order may be granted for up to 60 days. In the case of criminal organizations and terrorism offences, the order may be granted for up to one year (Section 186.1). Sections 186(6) and 186(7) provide for the renewal of an authorization. A renewal is granted on the same criteria as the original order and may not be granted for a period longer than 60 days.

- the names of the persons who are the target of the authorization?  
  X Yes   ☐ No

Section 186(4)© provides that the authorization must state the identify of the persons who are the target of the authorization, if their identity is known at the time of the authorization.

2. Do legislative provisions require that the person whose communications have been intercepted be notified of this fact once the interception has ended?  X Yes   ☐ No

Section 196 of the Code provides that named persons whose communications were intercepted must be notified within 90 days of the expiry of the authorization. The Court can extend the notification period if the investigation is continuing, but the extension cannot be for more than 3 years. The usual reason for extending the notification period is that notifying the targets would frustrate the ongoing investigation.

**Topic II: The admissibility of intercepted communications in criminal trials**

3. Is some type of admissibility hearing held to determine whether evidence obtained through the electronic interception of communications may be admitted in evidence against an accused person at his/her trial?  X Yes   ☐ No

4. Is the accused in preparation for his/her criminal trial permitted to review all evidence that was presented at the initial request or application for an authorization?  X Yes   ☐ No

Under Section 187(1.4) of the *Criminal Code*, the accused can apply to a judge for an order allowing him/her to review the evidence presented at the initial application in order to prepare for trial. However, before the accused can review the evidence, the prosecuting attorney is allowed to delete any information that the prosecution believes could: i) compromise the identity of any confidential informant; ii) compromise the nature and extent of an ongoing investigation, iii) endanger persons engaged in particular intelligence gathering techniques, or iv) prejudice the interests of innocent persons.

5. Is the accused’s counsel permitted to question the persons who prepared written or made oral statements at the initial request or application for an authorization?  X Yes   ☐ No
If yes, are there criteria used by the Court to permit this questioning? **X Yes**  □ No  
If yes, what are the criteria?

The accused will be allowed by the Court to question the person who made the statements at the initial application for an authorization if the Court is satisfied that the questioning is necessary to enable the accused to make full answer and defence. The accused must show a basis for the position that the questioning will elicit testimony tending to discredit the existence of one of the pre-conditions or criteria required for the approval of the authorization by the Court. The questioning cannot turn into a “fishing expedition” by the accused.

6. For what reasons would a Court not permit the use of intercepted private communications in a criminal prosecution?

The Court would refuse to permit the use of the intercepted communications in a criminal prosecution if the authorization order initially granted breached the constitutional right against unreasonable search or seizure. An authorization order would breach the right against unreasonable search or seizure if there was not enough evidence to support the order. However, even if the communications were intercepted in an unlawful or unconstitutional manner, the intercepted communications may still be admissible pursuant to Section 24(2) of the *Canadian Charter of Rights and Freedoms* (the “Charter”). Under Section 24(2) of the Charter, the applicant would have to demonstrate that:

i) the applicant’s *personal* Charter right was infringed;

ii) that the evidence was obtained in a manner that infringed the applicant’s Charter right; and

iii) having regard to all the circumstances, the admission of the evidence would bring the administration of justice into disrepute.

The seriousness of the constitutional breach is the most significant factor in determining whether illegally obtained interceptions or communications should be admissible. As interception of communications is only allowed in relation to serious offences, the exclusion of the intercepted communications is infrequent, because the application of the administration of justice principles usually renders the intercepted communications admissible.

Some examples of cases where Canadian Courts have not permitted the use of intercepted private communications include:

- where the intercepted communications were obtained after entering residential premises, where the order did not specifically allow entry into residential premises;

- where the accused was known to be a person whose private communications might assist in the investigation and the accused was not named in the authorization;
Would the Court refuse to permit the use of intercepted private communications depending on the profession of the person to whom the communication is made (ie. lawyer, priest, doctor) or the legal relationship between the persons whose communication has been intercepted (ie. spouse)? **X Yes**  □ No

Explain.

Section 186(2) of the *Criminal Code* imposes strict limitations on the interception of communications between a lawyer and a client. An authorization to intercept communications be a lawyer and client can be given only when the Court is satisfied that there are reasonable grounds to believe that the lawyer has been, or is about to be a party to a criminal offence. A Court may authorize the interception of communications at the office or residence of a lawyer if there are reasonable grounds to believe that the employees of the lawyer or members of the lawyer’s household have been or are about to be parties to a criminal offence. Even where the communication between a lawyer and a client is intercepted lawfully, the communication may still be protected by solicitor-client privilege rendering it inadmissible. Section 189 of the *Criminal Code* provides that any information obtained by an interception that, but for the interception, would have been privileged, remains privileged and inadmissible.

Similarly, while a judge may authorize the interception of communications between a husband and a wife, the communications are not admissible in Court because they are privileged. However, a judge may still authorize the interception of communications between a husband and a wife as such communications may provide assistance in the investigation process.

With respect to doctors and religious communications, there is a presumption that such communications are admissible, unless the following criteria, known as the Wigmure criteria, are met:

1) the communications must originate in a confidence that they will not be disclosed;

2) this element of confidentiality must be essential to the full and satisfactory maintenance of the relation between the parties;

3) the relation must be one which in the opinion of the community ought to be sedulously fostered;

4) the injury that would inure to the relation by the disclosure of the communications must be greater than the benefit thereby gained for the correct disposal of litigation.

**Can the Court refuse to admit evidence such as drugs and cash seized as a result**
of an unlawful interception of a private communication?  X Yes  □ No

Yes, however even in circumstances where the interception of private communications was unlawful, the evidence obtained as a result of the unlawful communication may still be admitted under Section 24(2) of the Charter if its admission does not bring the administration of justice into disrepute (please see answer to Question 6).

7. In your country, are there domestic legislative provisions or international conventions that regulate the interception of private communications by foreign investigative agencies (ie. CIA, DEA)?  □ Yes  X No  If yes, provide details.
There is no specific legislation empowering foreign agencies to intercept private communications within Canada. One might envisage a situation, however, in which Canadian policing authorities could co-operate with foreign agencies in the investigation and prosecution of transnational crime. Canadian authorities would still need to meet the requirements of the Criminal Code for obtaining an authorization.

Many thanks for completing the questionnaire. All responses will be tabulated and discussed at our October, 2009 meeting in Marrakech.