REPORT OF THE THIRD STUDY COMMISSION
THE INTERCEPTION OF COMMUNICATIONS
AND ITS IMPACT ON PRIVACY RIGHTS
International Association of Judges
Marrakech, Morocco
October 11-15, 2009

I. INTRODUCTION

At its 2009 annual meeting, the Third Study Commission examined the use in member countries of electronic devices as a criminal investigation tool to intercept private communications. The questionnaire circulated to member countries prior to the meeting explored the conditions under which the electronic interception of private communications is authorized and the legal principles that apply to the admissibility of evidence derived from the interception of communications.

II. QUESTIONNAIRE RESULTS & DISCUSSION

The Commission received 35 responses to the questionnaire. Delegates from over 25 countries participated in the two Study Commission sessions and provided valuable contributions to our discussions. Small group discussions were included in each session, along with a program evaluation form. While the questionnaire was more wide-ranging than what is contained in this report, general as well as unique trends have been selected for discussion. A chart summarizing the questionnaire responses is annexed to this report.

Generally, member countries protect the rights of an accused person with regard to electronic interception of communications. Surveillance usually requires prior judicial authorization, and appears to be an exceptional measure limited to serious crimes and for the most part, is authorized for a limited period of time.

A. The Initial Authorization Application

i. Special Legislation for Interception

All member countries who responded have adopted special legislation authorizing the interception of private communications to assist in the investigation of crime. A majority of questionnaire responses reported that interception requires prior authorization by a court. England is a notable exception. There the authorization is signed by senior police officials. In civil law member countries such as Belgium, France, and the Netherlands, the *juge d'instruction* authorizes the interception.

In some member countries, judicial authorization is not required where a time delay would impair the investigation. For example, in Norway, Taiwan, and Germany, the public prosecutor can authorize interception, however, the order must be confirmed by a court as soon as possible (within 24 to 72 hours). In Canada, the *Criminal Code* permits interception of private communications without prior court authorization where the police officer believes that: the situation is so urgent that authorization could not be obtained in the usual manner and the interception is necessary to prevent an unlawful act that would seriously harm a person or property. The United States of America has a similar exception for emergency circumstances.

In Austria, acoustical surveillance does not require prior court authorization in situations where: a kidnapping is suspected, the surveillance is restricted to comments made at the time and location of the kidnapping, and is restricted to comments made in public places or in the presence of an investigator and is used to prevent dangerous attacks against persons or property.

ii. Conditions or Criteria Required for Judicial Authorization

Generally, the responses indicated that interception of private communications is limited to serious crimes, *i.e.* where the suspected offences carries a longer term of imprisonment, although the term varied from one to eight years among member countries. "Serious" crimes include: murder, kidnapping, robbery, sexual assault, fraud, human or drug trafficking, and child pornography. Most member countries reported that before an authorization is granted, a judge will require sufficient circumstantial evidence of the crime as well as evidence, in several countries, that the surveillance is necessary or that the investigation cannot be carried out in another way.

iii. Nature of the Application

In a great majority of member countries, either a police officer or a public prosecutor submits a written application to the judge who then provides a written response (Germany, Croatia, Estonia, Luxembourg, Slovenia, and Taiwan, for example). In Brazil, the judge has twenty-four hours to grant or deny the application. In Slovenia and Hungary, the time period is slightly longer at forty-eight hours and seventy-two hours, respectively.

In Canada, the U.S.A. and Australia, the supporting evidence is presented in the form of a sworn written statement. In Denmark, Finland and Slovenia, the hearing proceeds on the basis of *viva voce* evidence. In the U.S.A., a hearing is conducted, however, the evidence relied upon is sworn and in writing.

In Belgium, the Netherlands and France, for example, the investigating judge authorizes the interception and directs the entire investigation, overseeing the legality of the evidence, requesting the services of the police where needed, and determining which communications, once gathered, are relevant to the investigation.

Every member country in which *viva voce* hearings are held, aside from Brazil, indicated that application hearings for interception are not audio-recorded. In Brazil, the hearing is recorded and transcribed. It was suggested that where evidence is in oral form, some means of recording would be beneficial to ensure transparency and the existence of a record of the application. In Australia, the applicant must disclose any possible effects on the privacy of persons other than the target.

Interest was expressed in a procedure adopted in some countries to ensure transparency in the application for authorization process. A third party attends the application for the interception, who essentially acts as a "contradictor" of the officer or prosecutor's position and is variously referred to as a monitor in Queensland, Australia, an ombudsman in Sweden, and simply as a lawyer in Denmark and Norway. This third party monitors compliance with procedural rules

and injects some transparency and quality control into the very first stage of the interception process.

iv. Nature and Duration of the Authorization

In all member countries who responded, except Belgium and Latvia, the authorization order must specify the types of interception devices to be used. In the United States of America, the authorization must specify the kind of communication to be intercepted but need not specify what types of surveillance may be used.

Generally, the responses indicated that the authorization is of limited duration. The length of time varied from 1 to 4 months with the possibility of extension or renewal for an equivalent time period. In Austria, there is no maximum time limit; interception may be ordered for the period of time required to fulfill the purpose of the investigation. England does not require the length of time to be specified.

Almost all member countries require the name of the persons who are the target of the interception (if their identity is known) to be included in the authorization. The Netherlands does not require that a name be provided, but does require that the authorization be as complete as possible.

v. Requirement of Notice to Party Intercepted

A majority of the member countries who responded require the intercepted party who is not subsequently charged with an offence to be notified of the interception once it has ended, unless doing so would jeopardize the investigation. However, Australia, Brazil, England, France, Georgia, Israel, Norway, and Spain do not have legislative provisions that require notification. In Norway, it is only upon an application being made that a person is informed whether he/she was the subject of an electronic interception.

B. The Admissibility of Intercepted Communications

i. Holding of Admissibility Hearing

In most member countries, there is an opportunity afforded either before or at trial to determine whether evidence obtained through interception may be admitted as evidence against the accused. at trial. For example, in Austria and Germany, such evidence may be challenged by the accused at any stage of the proceedings, including before or after the introduction of the evidence at trial and on appeal.

ii. Extent of Review of Evidence

Most member countries permit the accused to review the evidence that was presented at the initial interception application. However, in these same countries, either the prosecution (Austria) or the judge (Belgium) has discretion to edit out information that could compromise the proceedings or an ongoing investigation. In Canada, the prosecution can withhold information from the accused that could compromise the identity of an informant or prejudice the interests of innocent persons.

iii. Questioning Witnesses

A vast majority of member countries permit the questioning by defence counsel, at or before trial, of officers who were involved with the initial interception application. In Canada, however, questioning is limited to the extent that it will show the absence of one of the pre-conditions or criteria that was required for the initial court authorization. In Japan and Germany, such questioning must be relevant to the authorization, such as a witness' credibility, while in England there can be a withholding of information by reason of public interest immunity. In the U.S.A., the law neither specifies discovery procedures nor imposes limits on the discovery rights of persons whose communications have been intercepted.

In Taiwan, if the validity of the authorization is disputed, a hearing is held in which counsel for the accused can subpoena witnesses to challenge the factual basis for the surveillance.

In Austria, Belgium and Switzerland, counsel for the accused cannot question the witnesses. In Belgium, the accused is interrogated by the presiding judge. During his pleading, the accused can dispute the validity of the surveillance on the basis that it was unlawfully granted and the evidence produced from the surveillance is excluded. In Switzerland, defence counsel can access the court file prior to trial, but cannot cross-examine witnesses on its contents.

iv. Basis for Refusal to Admit Evidence

There is a significant difference between common-law and civil law jurisdictions regarding the admission of evidence derived from intercepted conversations. The focus in civil law jurisdictions is on compliance with procedural rules, whereas in common-law jurisdictions, the court may consider whether there were irregularities in the substantive evidence before the authorizing judge.

Some member countries recognize an overarching right of privacy within communications with lawyers, doctors, priests, and spouses (Hungary, Slovenia, Finland and the U.S.A.), lawyers, doctors, and priests (Israel, Japan, and Latvia) while other countries limit it to lawyers and doctors (Belgium), lawyers and spouses (Canada), lawyers and Parliamentarians (England), or do not recognize a privacy right at all (Brazil, Georgia, and Taiwan).The privacy of the communication will be lost if the suspect is using the office, residence, or telecommunications network of the professional to commit an offence.

The responses also varied as to whether a court would permit the admission of evidence seized as a result of an unlawful interception. Austria, Estonia, and Germany would admit such evidence while France, Georgia, Hungary, Ireland, Israel, Japan, the Netherlands, Norway, Slovenia, Spain, Switzerland, Taiwan, and the U.S.A., in certain circumstances, would not. Belgium, Latvia, and Canada had more equivocal responses. Under Latvian law, any evidence obtained by violence, fraud or duress or in violation of criminal procedure is inadmissible. However, information obtained by other procedural violations is restrictedly admissible where such violations did not influence the veracity of the information or the reliability of the information is proved by other information in the proceedings. Finally, in Canada, unlawfully obtained evidence may be declared inadmissible if the accused can show: that his personal right was infringed; the evidence was obtained in a manner that infringed his right; and the admission of the evidence would bring the administration of justice into disrepute.

In Finland, if information from an interception is used in another investigation, the legal test is: "After having carefully evaluated all the facts presented, the court shall decide what is regarded as the truth in the case." With regard to the fruits of unlawful interception, Finnish law follows the principle of "free assessment of evidence," such that even unlawfully intercepted communication is admissible. The court then decides the probative value of the evidence. However, because the communication was obtained unlawfully, the officer who carried out the interception would be considered to have committed an offence and would be the subject of a criminal investigation.

v. Foreign Requests for Interception

Almost all of the member countries indicated that they have no domestic legislative provisions or international conventions governing the interception of private communications by foreign investigative agencies. Most member countries stated that they would cooperate with foreign agencies in the investigation and prosecution of transnational crime, however, foreign agencies must comply with domestic laws.

Belgium was one of the few member countries to indicate special domestic legislation governing the interception of private communications by foreign agencies. The Belgian *Criminal Code* explicitly permits a foreign authority to effect a wiretap or be apprised of telecommunications relating to persons on Belgian territory if: the wiretap does not involve the technical intervention of anyone in Belgium; the foreign state has advised authorities; the measure is authorized by an international treaty between Belgium and the foreign state; and it is likely that a Belgian *juge d'instruction* would authorize the wiretap.

The United States of America also has domestic legislation, namely the *Foreign Intelligence Surveillance Act* (FISA) governing foreign requests fro interception. FISA prescribes procedures for the electronic and physical surveillance and collection of foreign intelligence information between foreign powers and agents of foreign powers on U.S. soil. Under the legislation, the President of the United States may permit interception of communications by foreign agencies without a court order for periods of up to one year. FISA also created the Foreign Intelligence Surveillance Court (FISC) to hear applications for orders approving the electronic surveillance of foreign intelligence agents inside the U.S.; a denial of an application by FISC may be appealed to the Court of Review. FISA was amended in 2001 to include terrorist groups that exist separate and apart from foreign governments.

III. TOPIC FOR 2010

The topic chosen for next year's questionnaire and conference is Human Trafficking.

IV. USE OF STUDY COMMISSION REPORTS

We wish to note the valuable information contained in the reports released each year from the four Study Commissions. The Third Study Commission recommends that steps by taken by the Central Council to develop effective channels of communication of these annual Study Commission reports to the U.N., to N.G.0's that help countries develop judicial institutions, and to academic researchers.

V. INTERPRETATION SERVICES

We very much appreciated the consecutive form of interpretation (English to French and French to English) provided at both our plenary sessions this year. We hope that interpretation services will be provided for our Study Commission meetings next year given the participation of a large number of francophone delegates at our meetings.

VI. STUDY COMMISSION OFFICERS

The officers re-elected at the annual 2008 meeting for a further two-year term are: President: Mary Moreau (Canada); Vice-Presidents: Frans Bauduin (Netherlands) and Messey Momble (Ivory Coast).

Respectfully submitted,

_____

Mary Moreau
President - Third Study Commission
October 15, 2009