IN THE MATTER OF an application by [portion deleted by order of the Court] for a warrant pursuant to Sections 12 and 21 of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23;

AND IN THE MATTER OF [portion deleted by order of the Court]

INDEXED AS: X (RE) (F.C.)

Federal Court, Mosley J.—Ottawa, October 5, 2009.

Security Intelligence — Application for warrant authorizing use of intrusive investigative techniques with respect to threat-related activities of Canadian citizens outside Canada under Canadian Security Intelligence Act (Act), s. 21 — Authorization sought for interception of communications, seizure of information by Canadian Security Intelligence Service (CSIS) with assistance of Communications Security Establishment (CSE) — Proposed interceptions would be controlled from within Canada — Whether Court having jurisdiction to authorize acts by CSIS in this country entailing listening to communications, collecting information obtained from abroad — Judge having jurisdiction, under Act, s. 21, to authorize CSIS to intercept communications, obtain information, carry out activities necessary to achieve these purposes — No geographical limitation in Act restricting interception of communications to those originating, intended to be received in Canada — Here, interceptions to take place at locations within Canada where calls acquired, listened to, recorded — Reasoning of U.S. Circuit Courts of Appeals holding judge having jurisdiction to authorize interception if first location at which communications listened to within judge's territorial jurisdiction persuasive — Court having jurisdiction to issue warrant herein — Collection of information by CSIS with CSE assistance falling within legislative scheme approved by Parliament — Application allowed.

Federal Court Jurisdiction — Application for warrant authorizing use of intrusive investigative techniques with respect to threat-related activities of Canadian citizens outside Canada under Canadian Security Intelligence Act (Act), s. 21 — Powers sought to intercept, seize information possibly having extra-territorial impact — If location of intercept construed as occurring abroad, Court having no jurisdiction to issue warrant authorizing activities — Here, interceptions to take place at locations within Canada where calls acquired, listened to and recorded — Court having jurisdiction to issue warrant authorizing CSIS, with technical assistance of CSE, to listen to, record communications at location within Canada.

International Law — Application for warrant authorizing use of intrusive investigative techniques with respect to threat-related activities of Canadian citizens outside of Canada — Whether Court may authorize action in Canada knowing collection of such information in foreign country may violate state's territorial sovereignty — What was proposed in present warrant not constituting enforcement of Canada's laws abroad but rather exercise of jurisdiction here relating to protection of Canada's security — While norms of territorial sovereignty precluding exercise of nation's enforcement jurisdiction in territory of another nation, not precluding collection of information.

Constitutional Law — Charter of Rights — Unreasonable Search or Seizure — Application for warrant authorizing use of intrusive investigative techniques with respect to threat-related activities of Canadian citizens outside of Canada — Ample grounds herein for interfering with privacy interests of individuals concerned, no issue arising as to whether collection of information would breach rights to protection against unreasonable search, seizure — As statutory prerequisites of warrant met, collection of information by CSIS with CSE assistance falling within legislative scheme approved by Parliament, not offending Charter.

These were the reasons for the issuance of a warrant authorizing the use of intrusive investigative techniques with respect to threat-related activities of two Canadian citizens outside of Canada under section 21 of the *Canadian Security Intelligence Act* (Act). Authorization was sought for the interception of communications and the seizure of information by the Canadian Security Intelligence Service (CSIS) with the assistance of the Communications Security Establishment (CSE).

Section 12 of the Act provides that CSIS shall collect, analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of

Canada. These include activities within or relating to Canada. Under section 21, a judge has jurisdiction to authorize CSIS to intercept communications and obtain information and to carry out the activities necessary to achieve those purposes.

The issue was whether the Court had jurisdiction to authorize acts by CSIS in this country which entailed listening to communications and collecting information obtained from abroad.

Held, the application should be allowed.

CSIS sought to listen to, record or acquire communications between the places of their origination and destination. There is no geographical limitation in the Act restricting the interception of communications to those which either originate or are intended to be received in Canada. While the interception of communications which are being transmitted would appear to present little difficulty from a jurisdictional perspective so long as the signals are intercepted from within Canada, of greater concern were the proposed powers to intercept and seize information that may have an extraterritorial impact. This gave rise to a concern about where the communication is intercepted within the meaning of the statute. If the location of the intercept was to be construed as occurring abroad, the Court, applying the principles set out by Blanchard J. in *Canadian Security Intelligence Service Act (Re)*, would have no jurisdiction to issue a warrant authorizing such activities. In the present context, the interceptions were to take place at the locations within Canada where the calls would be acquired, listened to and recorded. While there appears to be no Canadian case law directly on point, the U.S. Circuit Courts of Appeals have held that a judge has jurisdiction to authorize the interception of communications if the first location at which they will be listened to is within the judge's territorial jurisdiction. They have interpreted "interception" to include both the place where the telephones which are the subject of judicial warrants are located and the place where the communications are first heard by law enforcement officials. This reasoning was found to be persuasive.

The Court had jurisdiction to issue a warrant authorizing CSIS, with the technical assistance of CSE, to listen to and record communications at a location within Canada. In doing so, the Court was not authorizing CSE to overstep its legislative mandate as set out under the *National Defence Act*. CSE would not be directing its activities at Canadian citizens to acquire information for its purpose, which it is prohibited from doing under paragraph 273.64(2)(*a*) of this statute. It would be assisting CSIS under paragraph 24(*b*) of the *Canadian Security Intelligence Act.*

A seizure, within Canada, of information in which the holder has a reasonable expectation of privacy invokes section 8 of the Charter. In the present case, there were ample grounds for interfering with the privacy interests of the individuals concerned and no issue arose as to whether the collection of the information would breach the individuals' rights to protection against unreasonable search and seizure. The question was whether the Court could authorize this action in Canada knowing that the collection of such information in a foreign country may violate the state's territorial sovereignty. There were sufficient factual and legal grounds to distinguish the application from that which was before Justice Blanchard. What was proposed in the present warrant did not constitute the enforcement of Canada's laws abroad but rather the exercise of jurisdiction here relating to the protection of Canada's security. While the norms of territorial sovereignty preclude the exercise of a nation's enforcement jurisdiction in the territory of another nation, they do not preclude the collection of information. CSE has a mandate to collect foreign intelligence including information from communications and from technology systems and networks abroad. It is restricted from directing its activities against Canadians or any person within Canada, but it is not constrained from providing assistance to security and law enforcement agencies acting under lawful authority. As the statutory prerequisites of a warrant (prior judicial review, reasonable grounds, particularization of the targets) were met, the collection of information by CSIS with CSE assistance fell within the legislative scheme approved by Parliament and did not offend the Charter.

STATUTES AND REGULATIONS CITED

Anti-terrorism Act, S.C. 2001, c. 41.

Canadian Charter of Rights and Freedoms, being Part I of the *Constitution Act, 1982*, Schedule B, *Canada Act 1982*, 1982, c. 11 (U.K.) [R.S.C., 1985, Appendix II, No. 44], s. 8.

Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23, ss. 2 "intercept", "threats to the security of Canada" (as am. by S.C. 2001, c. 41, s. 89), 12, 21, 24, 26.

Criminal Code, R.S.C., 1985, c. C-46, s. 183 "intercept", "private communication" (as am. by S.C. 1993, c. 40, s. 1).

National Defence Act, R.S.C., 1985, c. N-5, s. 273.64 (as enacted by S.C. 2001, c. 41, s. 102).

Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 "intercept", 2518(3).

TREATIES AND OTHER INSTRUMENTS CITED

Convention on Cybercrime, 23 November 2001, 2296 U.N.T.S. 167, Eur. T.S. 185, preamble, Articles 2, 3, 4, 5, 32.

CASES CITED

DISTINGUISHED:

Canadian Security Intelligence Service Act (Re), 2008 FC 301, [2008] 4 F.C.R. 230.

CONSIDERED:

Canadian Security Intelligence Service Act (Re), 2008 FC 300, [2008] 3 F.C.R. 477; *R. v. Hape*, 2007 SCC 26, [2007] 2 S.C.R. 292, 280 D.L.R. (4th) 385, 220 C.C.C. (3d) 161; *Amnesty International Canada v. Canada (Chief of the Defence Staff)*, 2008 FC 336, [2008] 4 F.C.R. 546, 292 D.L.R. (4th) 127, 81 Admin. L.R. (4th) 190, affd 2008 FCA 401, [2009] 4 F.C.R. 149, 305 D.L.R. (4th) 741, 182 C.R.R. (2d) 203; *R. v. Taylor* (1997), 42 C.R.R. (2d) 371 (B.C.C.A.), affd [1998] 1 S.C.R. 26, (1998), 121 C.C.C. (3d) 353, 48 C.R.R. (2d) 372; *U.S. v. Denman*, 100 F.3d 399 (5th Cir. 1996); *Castillo v. Texas*, 810 S.W.2d 180 (Tex. Crim. App. 1990).

REFERRED TO:

Rizzo & Rizzo Shoes Ltd. (Re), [1998] 1 S.C.R. 27, 36 O.R. (3d) 418, 154 D.L.R. (4th) 193; *R. v. McQueen* (1975), 25 C.C.C. (2d) 262, [1975] W.W.R. 604 (Alta. C.A.); *R. v. Giles*, 2007 BCSC 1147; *R. v. Taillefer* (1995), 100 C.C.C. (3d) 1, 40 C.R. (4th) 287 (Que. C.A.); *U.S. v. Rodriguez*, 968 F.2d 130 (2d Cir. 1992); *U.S. v. Luong*, 471 F.3d 1107 (9th Cir. 2006); *U.S. v. Ramirez*, 112 F.3d 849 (7th Cir. 1997); *U.S. v. Jackson*, 471 F.3d 910 (7th Cir. 2000); *U.S. v. Tavarez*, 40 F.3d 1136 (10th Cir. 1994); *People v. Perez*, 848 N.Y.S.2d 525 (N.Y. Sup. Ct.); *Bell Canada Ltd. v. M.N.R.*, 2008 FCA 348, [2010] 1 F.C.R. 145, 53 B.L.R. (4th) 202, [2009] 2 C.T.C. 141; *In re: Sealed Case*, 310 F.3d 717 (F.I.S.C.R. 2002); *In re: Directives [Redacted Text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (F.I.S.C.R. 2008).

AUTHORS CITED

Currie, John H. *Public International Law*, 2nd ed. Toronto: Irwin Law, 2008.

Explanatory Report to the *Convention on Cybercrime*, 23 November 2001, Eur. T.S. 185, paras. 38, 58, online: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

Goldsmith, Jack L. "The Internet and the Legitimacy of Remote Cross-Border Searches" (2001), *U. Chi. Legal F.* 103.

University of Ottawa. *Canadian Internet Policy and Public Interest Clinic*, online: <http://www.cippic.ca/projects-cases-lawful-access/>.

Wilske, Stephan and Teresa Schiller. "International Jurisdiction in Cyberspace: Which States May Regulate the Internet?" (1997), 50 *Fed. Com. L.J.* 117.

APPLICATION for a warrant authorizing the use of intrusive investigative techniques by the Canadian Security Intelligence Service with the assistance of the Communications Security Establishment with respect to threat-related activities of Canadian citizens outside of Canada under section 21 of the *Canadian Security Intelligence Act*. Application allowed.

The following are the amended and redacted public reasons for order rendered in English by

[1] MOSLEY J.: On November 27, 2008 the Court issued warrants pursuant to sections 12 and 21 of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23 (the Act) with respect to the activities of two Canadian citizens whose activities, on reasonable grounds, were believed to constitute threats to the security of Canada. The warrants authorized the use of intrusive investigative techniques and information collection at locations within Canada for a term of one year.

[2] On January 24, 2009, an application was filed on urgent grounds seeking the issuance of an additional warrant against the same two individuals in respect of newly identified threat-related activities. The application was supported by the affidavit evidence of the applicant, an officer of the Canadian Security Intelligence Service (CSIS or the Service), and that of an expert employed by the Communications Security Establishment (CSE). A hearing was conducted on Saturday, January 26, 2009, at which oral evidence was heard together with submissions presented on behalf of the applicant by counsel for the Attorney General of Canada. Written submissions and authorities were also filed with the Court.

[3] This latter application differed from that dealt with in November 2008 in that it pertained to threat-related activities which, it was believed, the two individuals would engage in while traveling outside of Canada. In that respect, the application was similar to one heard and denied by Mr. Justice Edmond Blanchard in a decision rendered on October 22, 2007 (SCRS-10-07) and reported in an expurgated version in *Canadian Security Intelligence Service Act (Re)*, 2008 FC 301, [2008] 4 F.C.R. 230 [*CSIS (Re)*]. In that decision, Justice Blanchard held that the Court lacked jurisdiction under the Act to authorize intrusive investigative activities by CSIS employees outside of Canada.

[4] In the present matter, the Court was asked to revisit the question of jurisdiction and to distinguish Justice Blanchard's reasoning in the 2007 decision on the basis of:

a. a more complete description of the facts relating to the activities necessary to permit the interception of the communications and the procedures to be used to obtain the information sought; and

b. a different legal argument concerning how the method of interception is relevant to the jurisdiction of this Court.

[5] After reading the material before the Court and hearing the evidence of the CSE witness and the sub-missions of counsel, I was satisfied that there were sufficient factual and legal grounds to distinguish the application from that before Mr. Justice Blanchard and issued the warrant for a term of three months. On April 6, 2009, I heard further submissions from counsel and on April 16, 2009, I extended the warrant for a further nine months. I deem it appropriate at this time to provide my reasons in writing for issuing the warrant based on the application before me.

Background

[6] The issues addressed by Justice Blanchard in the 2007 application had first been presented to Mr. Justice Simon Noël on an application filed in June, 2005 (CSIS-18-05). In those proceedings, Justice Noël had appointed Mr. Ronald Atkey, Q.C. to serve as *amicus curiae*. A preliminary issue arose as to whether the questions of law raised by the application could be dealt with in a public hearing. Upon receiving written and oral submissions on that issue, Justice Noël concluded that the application should be conducted in private. His comprehensive reasons for that decision have been made public: *Canadian Security Intelligence Service Act (Re)*, 2008 FC 300, [2008] 3 F.C.R. 477. On August 23, 2006, a notice of discontinuance was filed in the matter by counsel for the Deputy Attorney General of Canada before a determination of the questions of law regarding the scope of the Court's jurisdiction could be addressed.

[7] The question of extraterritorial jurisdiction was then raised again in an application for warrants brought before Justice Blanchard in April 2007. He was satisfied on the basis of the affidavit evidence that the prerequisites referred to in paragraphs 21(2)(*a*) and (*b*) of the Act had been established, that is that the facts relied on by the deponent to justify the belief on reasonable grounds that warrants were required to investigate threats to the security of Canada, that other investigative methods had been tried and failed, or were unlikely to succeed, and that important information regarding the threats would not otherwise be obtained. Accordingly, warrants were issued by Justice Blanchard at that time for execution within Canada.

[8] At the time he issued the initial warrants in appli-cation SCRS-10-07, Justice Blanchard was not prepared to authorize investigative activities by the Service outside Canada, as requested, without further consideration. Accordingly, Mr. Atkey was again appointed to assist the Court as *amicus curiae* and Justice Blanchard received written and oral submissions from him and from counsel for the Deputy Attorney General of Canada. These submissions focused initially on two questions framed by the Court: whether CSIS has a mandate to undertake threat-related investigations outside of Canada and second, whether the Federal Court has jurisdiction to issue warrants authorizing such investigations.

[9] Additional questions were identified by Justice Blanchard following the release of the decision of the Supreme Court of Canada in *R. v. Hape*, 2007 SCC 26, [2007] 2 S.C.R. 292 respecting the application of the *Canadian Charter of Rights and Freedoms*, being Part I of the *Constitution Act, 1982*, Schedule B, *Canada Act, 1982*, 1982, c. 11 (U.K.) [R.S.C. 1985, Appendix II, No. 44], which came into force on April 17, 1982 (the Charter) to investigations conducted abroad by Canadian authorities. Further submissions were received from the *amicus* and counsel on those questions.

[10] In *Hape*, the Supreme Court affirmed the principles that legislation is presumed to conform to international law absent express statutory language to the contrary and that customary international law prohibited interference with the domestic affairs of other states. In that regard, paragraph 65 of the *Hape* decision is most instructive:

> The Permanent Court of International Justice stated in the *Lotus* case, at pp. 18-19, that jurisdiction "cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention"…. According to the decision in the *Lotus* case, extraterritorial jurisdiction is governed by international law rather than being at the absolute discretion of individual states. While extraterritorial jurisdiction — prescriptive, enforcement or adjudicative — exists under international law, it is subject to strict limits under international law that are based on sovereign equality, non-intervention and the territoriality principle. According to the principle of non-intervention, states must refrain from exercising extraterritorial enforcement jurisdiction over matters in respect of which another state has, by virtue of territorial sovereignty, the authority to decide freely and autonomously (see the opinion of the International Court of Justice in the *Case concerning Military and Paramilitary Activities in and against Nicaragua*, at p. 108). Consequently, it is a well-established principle that a state cannot act to enforce its laws within the territory of another state absent either the consent of the other state or, in exceptional cases, some other basis under international law…. This principle of consent is central to assertions of extraterritorial enforcement jurisdiction. [Emphasis added; citations removed.]

[11] As described by Justice Blanchard at paragraphs 29–31 of his reasons, the Service took the position that the statutory scheme under the Act provides the necessary authority for the Court to issue a warrant having extra-territorial effect. They did not seek judicial authorization to violate foreign law but acknowledged that was the likely effect of the activities for which authorization was sought. The *amicus* agreed with the Service that there is no territorial limitation on the activities of CSIS related to the collection, analysis and retention of information respecting threats to the security of Canada as set out in section 12 of the Act. Any application for a warrant under section 21 of the Act may extend to investigative activities of CSIS outside of Canada. However, in the submission of the *amicus*, the Service could not execute a warrant obtained under section 21 and exercise its information gathering powers in another country unless it had obtained the permission of the country where the targets were located or was a party to a treaty or agreement covering the use of its powers in that country.

[12] After a review of the Act and the principles of international law discussed by the Supreme Court in *Hape*, Justice Blanchard concluded that he was unable to construe the applicable provisions of the statute as providing the Court with the jurisdictional basis to issue a warrant for execution abroad.

[13] Applying the modern principle of statutory interpretation adopted by the Supreme Court of Canada in *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 S.C.R. 27, at paragraph 41, Justice Blanchard found that the investiga-tive powers sought in the application before him were not expressly authorized by the statute. Among the factors Justice Blanchard considered, at paragraph 39 of his reasons, was the absence of any express territorial limitation in sections 12 and 21 of the Act. While this, he noted, might allow for an inference to be drawn in respect to a mandate for CSIS to conduct certain activities extraterritorially, that inference was not sufficiently obvious to provide a basis to conclude that the Service had a clear mandate to conduct the activities sought to be authorized in the warrant in countries other than Canada and that the Court has jurisdiction to authorize such activities.

[14] In light of his conclusion that he was unable to attribute a plain (or sufficiently clear, meaning to the provisions to permit extraterritorial application, Justice Blanchard then considered additional factors to assist in interpreting the intent of the legislation. In the result, he concluded that the evidence was insufficient to permit an inference to be drawn that Parliament intended the Service to be provided with a mandate to conduct investigative activities in the nature of those contemplated in the warrant then sought to be authorized.

[15] Justice Blanchard then proceeded to consider principles of international law. He found that the investigative activities for which authorization was sought would be likely to violate the laws of the jurisdictions where the warrant was to be executed. Absent the consent of the foreign states concerned to the application of Canadian law within their borders, the proposed investigative activities would breach their territorial sovereignty and violate customary international law.

[16] Justice Blanchard considered whether the *Criminal Code* of Canada, R.S.C., 1985, c. C-46 (the *Criminal Code*) and the Charter applied to the activities of CSIS agents conducting threat-related investigations outside of Canada. This portion of his reasons was not strictly necessary to his decision as Justice Blanchard had deter-mined the jurisdictional issue on the basis of statutory interpretation and international law principles.

[17] The Service's main contention in the application before Justice Blanchard was that the warrant sought was required to ensure that Canadian agents engaged in executing the warrant abroad do so in conformity with Canadian law since the impugned investigative activities may, absent the warrant, breach the Charter and contravene the *Criminal Code*. Section 26 of the CSIS Act provides that Part VI of the *Criminal Code* does not apply in relation to any interception of a communication under the authority of a warrant issued under section 21 of the Act. Absent this protection, Part VI would apply to the interception of any "private communication" as defined by section 183 [as am. by S.C. 1993, c. 40, s. 1] of the *Criminal Code*, that is any private communication where either the originator or the recipient was in Canada.

[18] Justice Blanchard found that the principles set out in *Hape* with respect to investigative jurisdiction in the context of criminal matters applied equally to the collection of information in the intelligence context. He concluded that the Charter could not be applied to the activities of intelligence officers collecting information abroad absent the consent of the foreign state concerned.

[19] I note that Madam Justice Anne Mactavish considered the application of the Charter in the distinct context of Canada's participation in the multinational military operation currently underway in Afghanistan in the case of *Amnesty International Canada v. Canada (Chief of the Defence Staff)*, 2008 FC 336, [2008] 4 F.C.R. 546, affd 2008 FCA 401, [2009] 4 F.C.R. 149. Applying the *Hape* principles, and in the absence of consent by the government of Afghanistan to the operation of Canadian law in their territory, Justice Mactavish held that the Charter did not apply to non-Canadian individuals detained by the Canadian forces in that country and transferred to the Afghan authorities.

Justice Mactavish observed, however, at paragraph 344 of her reasons that Canadian military personnel could face criminal prosecution under Canadian law for their actions in Afghanistan.

[20] In the present matter, I was satisfied that a warrant was justified and that there were exigent circumstances with respect to the nature of the threat which required that it be issued on an urgent basis. When I dealt with the application on January 26, 2009, I considered whether it would be appropriate to appoint *amicus curiae*, as had been done by Justices Noël and Blanchard, to assist the Court with the jurisdictional question. Given the urgency of the situation laid before me and the facts and legal argument presented on behalf of the applicant, I deter-mined that it would be inappropriate to delay the issuance of the warrant. Moreover, the question of whether extraterritorial warrant execution could be authorized had been thoroughly canvassed in the proceedings before Justice Blanchard.

Legislative Framework

[21] The relevant legislation is set out in the annex to these reasons. In summary, section 12 of the Act outlines the Service's mandate and provides that it shall collect, by investigation or otherwise, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. The service is required to advise and report to the government in respect of such activities.

[22] A judge acting under section 21 of the Act has the jurisdiction to authorize CSIS to intercept communications and to obtain information and to carry out the activities necessary to achieve those purposes. Prerequisites are that CSIS is investigating a "threat to the security of Canada"; that there are reasonable grounds to believe that a warrant is required; and that without the warrant, information of importance will not be obtained.

[23] "Threats to the security of Canada" are defined at section 2 [as am. by S.C. 2001, c. 41, s. 89] as including "activities within or relating to Canada directed toward or in support of the threat" (emphasis added).

[24] Under paragraph 21(2)(*f*) of the Act, an application for a warrant must also include a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given.

[25] The Act defines "intercept" in section 2 as having the same meaning given to that term in section 183 of the *Criminal Code*, which includes to "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof". As set out in section 26 of the Act, Part VI of the *Criminal Code* does not otherwise apply to interceptions made pursuant to a warrant issued under the Act.

Issue

[26] In essence, the argument put forward by the applicant is that this Court has jurisdiction under section 21 of the Act to issue warrants to ensure judicial control over activities by government officials in Canada in relation to an investigation that will extend beyond Canadian borders. The applicant concedes that the acts for which authorization is sought may violate the *Criminal Code* or the constitutional rights of individuals if not judicially approved.

[27] The issue to be determined is whether the Court has jurisdiction to authorize acts by CSIS in this country which entail listening to communications and collecting information obtained from abroad.

The Applicant's Case

[28] In the application before me authorization is sought for two types of activities: the interception of communications; and the seizure of information [portion deleted by order of the Court]. If granted, CSIS proposes to enlist the assistance of the CSE under paragraph 24(*b*) of the Act. Paragraph 24(*b*) provides that a warrant issued under section 21 may authorize any other person to assist a person acting in accordance with the warrant. With that assistance, CSIS proposes to intercept the following types of communications:

a. communications carried over [portion deleted by order of the Court];

b. communications that [portion deleted by order of the Court];

c. communications that [portion deleted by order of the Court].

[29] In addition to these communications, authorization is sought to obtain information [portion deleted by order of the Court].

[30] The applicant submits that the acts necessary to permit the interception of communications and to obtain information [portion deleted by order of the Court], with the technical assistance of CSE, will take place entirely in Canada. The communications will be heard, or the information obtained [portion deleted by order of the Court] will be read, only in Canada.

[31] CSE's mandate is set out in the *National Defence Act*, R.S.C., 1985, c. N-5, as amended by the *Anti-terrorism Act*, S.C. 2001, c. 41. Under paragraph 273.64(1)(*a*) [as enacted by S.C. 2001, c. 41, s. 102] of this statute, the agency is authorized to acquire and use information from the global information infrastructure (i.e., communications systems, information technology systems and networks) for the purpose of providing foreign intelligence to the Government of Canada. CSE is prohibited under paragraph 273.64(2)(*a*) [as enacted *idem*] from directing these activities at Canadian citizens and permanent residents wherever located (Canadian persons) or at any person in Canada regardless of nationality.

[32] The limitation respecting Canadian persons or persons in Canada does not apply to technical and operational assistance which CSE may provide to federal law enforcement and security agencies in the performance of their lawful duties pursuant to paragraph 273.64(1)(*c*) [as enacted *idem*] of the *National Defence Act*. Subsection 273.64(3) [as enacted *idem*] of this statute provides that such assistance activities are subject to any limitations imposed by law on the federal agencies in the performance of their duties.

[33] In the context of the present application, therefore, CSE may only assist CSIS to intercept communications and obtain information if CSIS has a judicially authorized warrant issued under section 21 of the Act.

[34] The evidence received from a CSE witness on January 26, 2009 described the agency's interception capabilities [portion deleted by order of the Court]. The evidence was that the proposed interceptions of communications would be controlled from within Canada [portion deleted by order of the Court].

[35] Telecommunications that can be intercepted or obtained by CSE from within Canada [portion deleted by order of the Court].

[36] [Portion deleted by order of the Court] every activity that affects the ability to intercept will take place in Canada. In those circumstances, counsel for the Deputy Attorney General submits, no issue of this Court's jurisdiction to issue the warrant arises.

[37] [Portion deleted by order of the Court]. The applicant's position is that [portion deleted by order of the Court] communications would be intercepted, within the meaning of the statute, solely where they would be listened to, that is within Canada.

[38] [Portion deleted by order of the Court]. Information found [portion deleted by order of the Court] would only be "seized" where it would be first read, in Canada.

[39] [Portion deleted by order of the Court.]

[40] The applicant submits that the matter of where a warrant is to be executed depends on where the telecom-munications will be intercepted and the information obtained. What is sought from the Court in this instance, it is submitted, is not a warrant that authorizes activities abroad but one which authorizes investigative activities to be conducted in Canada which will allow for com-munications to be listened to and information obtained from Canada.

[41] [Portion deleted by order of the Court.]

Analysis

Interception of Communications

[42] In considering this application, in addition to the evidence and submissions received, I had the benefit of being able to review Justice Blanchard's decision in its expurgated and non-expurgated forms and the content of the application that was before him. At paragraphs 14 through 16 of his reasons for decision, Justice Blanchard describes the nature of the warrant powers sought. Authorization was requested to intercept telecommunica-tions, to obtain information or records relating to the targets [portion deleted by order of the Court].

[43] The 2007 warrant application before Justice Blanchard sought authority to install, maintain or remove anything required [portion deleted by order of the Court]. It is clear from the warrant application itself and from Justice Blanchard's reasons that this was intended to include the authority to [portion deleted by order of the Court] in the foreign jurisdictions in order to install the means by which the communications, information and records [portion deleted by order of the Court].

[44] The draft of the warrant submitted for approval before me differed from that which was before Justice Blanchard in several significant respects. [Portion deleted by order of the Court]. The proposed authority to intercept at any place outside Canada where the telecommunication could be intercepted was removed. The authorities to install, maintain or remove anything required to intercept or obtain information and to obtain access to, search for, examine and record the information were limited to "from Canada".

[45] In my view, all of the activities for which authorization of the interception of telecommunications is sought would come within the broad meaning of the term "intercept" as defined in the Act by reference to the *Criminal Code* definition. The Service seeks to listen to, record or acquire communications between the places of their origination and the places of destination. Such activities constitute an "intercept" as interpreted by jurisprudence in relation to the *Criminal Code* definition: *R. v. McQueen* (1975), 25 C.C.C. (2d) 262 (Alta. C.A.); *R. v. Giles*, 2007 BCSC 1147.

[46] The request to authorize the interception of communications [portion deleted by order of the Court] presented little difficulty in my view as the warrant would be executed [portion deleted by order of the Court] within Canada. There is no geographical limitation in the CSIS Act that restricts the interception of communications to those which either originate or are intended to be received in Canada such as there is under Part VI of the *Criminal Code*. Absent such a geographical requirement, there would seem to be no statutory impediment to the interception of such communications under the CSIS Act and indeed, such warrants have been previously issued by this Court. Again, I would

note that Part VI of the *Criminal Code* does not apply to any interception under the CSIS Act nor in relation to any communication so intercepted.

[47] The interception of communications which are being transmitted [portion deleted by order of the Court] would also appear to present little difficulty from a jurisdictional perspective so long as the signals are intercepted from within Canada. [Portion deleted by order of the Court.]

[48] Of greater concern are the proposed powers to intercept and [portion deleted by order of the Court] seize information that may have an extraterritorial impact (underlined words added for clarity in the redacted version).

[49] [Portion deleted by order of the Court]. This gives rise to a concern about where the communication is intercepted within the meaning of the statute. If the location of the intercept must be construed as occurring abroad, the Court, applying the principles set out in Justice Blanchard's decision, would have no jurisdiction to issue a warrant authorizing such activities.

[50] In the context of Part VI *Criminal Code* authorizations, the place of land-line interceptions, and accordingly the jurisdiction to authorize these interceptions, is usually considered to be synonymous with the place where the subject phone is located even if the actual intercept takes place at a phone company switching station some distance away. With the advent of mobile phone technology, that has proven to be problematic in light of the constant switching of the communication between transmission cells as the phone is moved from location to location.

[51] In *R. v. Taylor* (1997), 86 B.C.A.C. 224, the British Columbia Court of Appeal reversed a trial judge's decision that a cellular communication had been unlawfully intercepted at a solicitor's office, contrary to the terms of the authorization. The Court of Appeal held that, properly construed, the interception had taken place not at the solicitor's office but at the distribution centre for cellular calls where the calls had been acquired and recorded. The Court adopted the reasoning of the Quebec Court of Appeal in *R. v. Taillefer* (1995), 100 C.C.C. (3d) 1 to the effect that the place where a call originates (or is received) should not be confused with the location authorized for its interception. The Supreme Court of Canada affirmed the decision in *Taylor* without providing additional reasons: [1998] 1 S.C.R. 26.

[52] In the present context, the interceptions for which authorization is granted will take place at the locations within Canada where the calls will be acquired, listened to and recorded.

[53] While there appears to be no Canadian jurispru-dence directly on point, counsel for the Deputy Attorney General of Canada has directed my attention to a number of American decisions in which it has been held by U.S. Courts of Appeals that a judge has the jurisdiction to authorize the interception of communications where the first location at which the communication will be listened to is within the judge's territorial jurisdiction: *U.S. v. Denman*, 100 F.3d 399 (5th Cir. 1996); *U.S . v. Rodriguez*, 968 F.2d 130 (2d Cir. 1992); *U.S. v. Luong*, 471 F.3d 1107 (9th Cir. 2006); *U.S. v. Ramirez*, 112 F.3d 849 (7th Cir. 1997) *U.S. v. Jackson*, 471 F.3d 910 (7th Cir. 2000); *U.S. v. Tavarez*, 40 F.3d 1136 (10th Cir. 1994); *People v. Perez*, 848 N.Y.S.2d 525 (N.Y. Sup. Ct.) *contra*, *Castillo v. Texas*, 810 S.W.2d 180 (Tex. Crim. App. 1990).

[54] The U.S. Congress regulates electronic surveillance under Title III of the *Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. § 2510. Under that statute "intercept" is defined very similarly to the definition in Part VI of the *Criminal Code* of Canada. It means the "aural or other acquisition of the contents of any wire, electronic, or oral communications through the use of any electronic, mechanical, or other device." Under the U.S. federal legislation, intercepts may only be authorized within the territorial jurisdiction of the Court in which the judge is sitting (18 U.S.C. § 2518 (3)). U.S. states have adopted similar jurisdictional requirements.

[55] U.S. Circuit Courts of Appeals that have considered the matter have interpreted "interception" as used in Title III to include both the place where the telephones which are the subject of judicial warrants are located and the place where the communications are first heard by law enforcement officers/officials.

[56] [Portion deleted by order of the Court] the interception must also be considered to occur at the place where the [portion deleted by order of the Court] contents are first heard. In *Denman*, above, the Court found that the interception occurs in both the location where the signal is acquired and that in which it is first listened to and judges in both locations have jurisdiction.

[57] The Texas Court of Criminal Appeal reached a different conclusion in *Castillo*. In that case, the majority of the Court of Criminal Appeal was concerned about the risk of "judge shopping" if a broader interpretation were to be recognized. They found that the State legislature had deliberately and expressly enacted a "territorial restriction" which limited the jurisdiction to authorize interception to the particular district in which the listening device was located. In *Perez*, the Supreme Court of New York considered that the risk of forum shopping was not a significant concern and followed the federal authorities.

[58] The reasoning in [portion deleted by order of the Court] the [portion deleted by order of the Court] U.S. Circuit Courts of Appeals decisions is persuasive. The interception of private communications under Canadian law requires more than just the technical acquisition of the signal bearing the communication. There must be a listening to or other form of acquisition of the substantive content of the communication. The fact that a telecommu-nication may be [portion deleted by order of the Court] does not preclude the issuance of an authorization to intercept the communication within Canada.

[59] In authorizing CSIS, with the technical assistance of CSE, to collect information [portion deleted by order of the Court] intercepted in Canada, I am not authorizing CSE to overstep its legislative mandate under the *National Defence Act*. [Portion deleted by order of the Court] CSE will not be directing its activities at Canadian citizens to acquire information for its purposes but assisting CSIS. The question before me is whether the Court may authorize CSIS to listen to and record the communications at a location within Canada [portion deleted by order of the Court]. Having considered the matter, I am satisfied that the Court has the jurisdiction to issue such a warrant.

[Portion Deleted by Order of the Court]

[60] The applicant submits that, [portion deleted by order of the Court], the jurisdictional requirements for the issuance of a warrant under section 21 are satisfied where the authorization sought is to obtain information from within Canada. I agree. However, the question of whether the Court may authorize the Service to [portion deleted by order of the Court] involves additional con-siderations.

[61] Section 21 of the Act empowers a designated judge to authorize CSIS to intercept any communication or obtain any information, record, document or thing. [Portion deleted by order of the Court].

[62] [Portion deleted by order of the Court.]

[63] [Portion deleted by order of the Court.]

[64] [Portion deleted by order of the Court]. A seizure, within Canada, of information in which the holder has a reasonable expectation of privacy invokes section 8 of the Charter. In the present case, there are ample grounds for interfering with the privacy interests of the individuals concerned and no issue arises as to whether the collection of the information would breach their Charter rights to protection against unreasonable search and seizure. The question is whether the Court may authorize

such action in Canada knowing that the collection of such information in a foreign country may violate that state's territorial sovereignty.

[65] In *CSIS (Re)*, above, at paragraph 54, Justice Blanchard held that "[n]o other basis under international law" had been put before him to warrant displacing the principles of sovereign equality, non-intervention and territoriality. CSIS had argued that customary international practice as it relates to intelligence gathering operations in a foreign state constituted an exception to principles of territorial sovereignty. I would observe again that the application before Justice Blanchard contemplated intrusive activities in foreign jurisdictions [portion deleted by order of the Court] that are not being sought in the present application. Subsequent to the decision of Mr. Justice Blanchard, the Federal Court of Appeal has observed that information may notionally reside in more than one place: see *eBay Canada Ltd. v. M.N.R.*, 2008 FCA 348, [2010] 1 F.C.R. 145.

[66] I am satisfied that there are sufficient factual and legal grounds to distinguish this application from that which was before Justice Blanchard. What has been proposed in the present warrant does not, in my view, constitute the enforcement of Canada's laws abroad but rather the exercise of jurisdiction here relating to the protection of Canada's security.

[67] The question of whether international comity precludes the use of investigative measures having an extraterritorial effect arises most frequently in criminal matters. This is the area in which most disputes have arisen as it goes to the core of the jurisdictional competence implied in state sovereignty: John H. Currie, *Public International Law*, 2nd ed. (Toronto: Irwin Law, 2008), at page 332 *et seq*. Criminal investigation was the context in which the Supreme Court made the statement in paragraph 65 of *Hape*, quoted above, that "a state cannot act to enforce its laws within the territory of another state absent either the consent of the other state or, in exceptional cases, some other basis under international law."

[68] An example of international comity in criminal matters can be found in the development of the *Convention on Cybercrime*, Eur. T.S. 185, opened for signature by the Council of Europe on 23 November 2001 [see also 2296 U.N.T.S. 167] and brought into force on July 1, 2004. Canada participated in the development of the Convention and has signed but not as yet ratified the instrument.

[69] The Convention responds to new forms of criminal conduct which arose with the growth of the Internet. Police agencies found they were frustrated by their inability to investigate foreign-based attacks on domestic computer systems. In some cases, the police resorted to cross-border computer searches to obtain evidence to support a domestic prosecution or a request for extra-dition. Such actions are perceived to violate the territorial sovereignty of the country where the data is located, absent consent: see Stephan Wilske and Teresa Schiller, "International Jurisdiction in Cyberspace: Which States May Regulate the Internet?" (1997), 50 *Fed. Com. L. J.* 117.

[70] The object of the Convention is to promote effective means for dealing with cybercrime. It provides for the criminalization of certain offences relating to computers, procedural powers to investigate and prosecute such crimes, expedited preservation and disclosure of stored computer data, and mutual legal assistance. Trans-border access to stored computer data is permitted with consent or where the data is publicly available (Article 32).

[71] Canada has yet to ratify the Convention in part because the legislation required for the domestic implementation of the data preservation and disclosure measures has not been enacted due to concerns expressed about their potential impact on privacy interests: see for example [*Canadian Internet Policy and Public Interest Clinic*, online:] <http://www.cippic.ca/projects-cases-lawful-access/>.

[72] It is clear from the Explanatory Report adopted with the Convention (available online at <http:// conventions.coe.int/Treaty/en/Reports/Html/185.htm>) that the multilateral agreement is not intended to affect measures taken by the subscribing parties to protect their national security

(paragraphs 38 and 58). However, the Convention does not provide a means by which information may be collected abroad for national security purposes. Its focus is on the criminal misuse of computer systems.

[73] As the facts of the present application disclose, individuals who pose a threat to the security of Canada may move easily and rapidly from one country to another and maintain lines of communication with others of like mind. Information which may be crucial to prevent or disrupt the threats may be unavailable to the security agencies of this country if they lack the means to follow those lines of communication.

[74] The norms of territorial sovereignty do not preclude the collection of information by one nation in the territory of another country, in contrast to the exercise of its enforcement jurisdiction. As Professor Jack L. Goldsmith argues in "The Internet and the Legitimacy of Remote Cross-Border Searches" (2001), *U. Chi. Legal F.* 103, technological innovation has simply made it easier to do this without physically crossing borders.

[75] Canada has given CSE a mandate to collect foreign intelligence including information from communications and information technology systems and networks abroad. It is restricted as a matter of legislative policy from directing its activities against Canadians or at any person within Canada, but it is not constrained from providing assistance to security and law enforcement agencies acting under lawful authority such as a judicial warrant. CSIS is authorized to collect threat-related information about Canadian persons and others and, as discussed above, is not subject to a territorial limitation.

[76] Where the statutory prerequisites of a warrant are met, including prior judicial review, reasonable grounds and particularization of the targets, the collection of the information by CSIS with CSE assistance, as proposed, falls within the legislative scheme approved by Parliament and does not offend the Charter.

[77] In concluding, I would note that American courts have held that the collection of intelligence respecting the communications of U.S. citizens who are travelling abroad falls outside the protection afforded by the U.S. Constitution's Fourth Amendment warrant requirement: *In re: Sealed Case*, 310 F.3d 717 (F.I.S.C.R. 2002) [Foreign Intelligence Surveillance Court of Review]; *In re: Directives [Redacted Text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act* [551 F.3d 1004 (F.I.S.C.R. 2008)], August 22, 2008, released in redacted form on January 12, 2009. Given the concern for the interests of Canadian persons evidenced by Parliament, it is preferable that such activities be authorized with prior judicial scrutiny as in this case.

ANNEX

Canadian Security Intelligence Service Act

2. In this Act,

…

"intercept" has the same meaning as in section 183 of the Criminal Code;

…

"threats to the security of Canada" means

(*a*) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,

(*b*) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,

(*c*) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and

(*d*) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (*a*) to (*d*).

…

12. The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.

…

21. (1) Where the Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee may, after having obtained the approval of the Minister, make an application in accordance with subsection (2) to a judge for a warrant under this section.

(2) An application to a judge under subsection (1) shall be made in writing and be accompanied by an affidavit of the applicant deposing to the following matters, namely,

(*a*) the facts relied on to justify the belief, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16;

(*b*) that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (*a*) would not be obtained;

(*c*) the type of communication proposed to be intercepted, the type of information, records, documents or things proposed to be obtained and the powers referred to in paragraphs (3)(*a*) to (*c*) proposed to be exercised for that purpose;

(*d*) the identity of the person, if known, whose communication is proposed to be intercepted or who has possession of the information, record, document or thing proposed to be obtained;

(*e*) the persons or classes of persons to whom the warrant is proposed to be directed;

(*f*) a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given;

(*g*) the period, not exceeding sixty days or one year, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (5); and

(*h*) any previous application made in relation to a person identified in the affidavit pursuant to paragraph (*d*), the date on which the application was made, the name of the judge to whom each application was made and the decision of the judge thereon.

(3) Notwithstanding any other law but subject to the *Statistics Act*, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(*a*) and (*b*) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,

(*a*) to enter any place or open or obtain access to any thing;

(*b*) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or

(*c*) to install, maintain or remove any thing.

(4) There shall be specified in a warrant issued under subsection (3)

(*a*) the type of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained and the powers referred to in paragraphs (3)(*a*) to (*c*) authorized to be exercised for that purpose;

(*b*) the identity of the person, if known, whose communication is to be intercepted or who has possession of the information, record, document or thing to be obtained;

(*c*) the persons or classes of persons to whom the warrant is directed;

(*d*) a general description of the place where the warrant may be executed, if a general description of that place can be given;

(*e*) the period for which the warrant is in force; and

(*f*) such terms and conditions as the judge considers advisable in the public interest.

(5) A warrant shall not be issued under subsection (3) for a period exceeding

(*a*) sixty days where the warrant is issued to enable the Service to investigate a threat to the security of Canada within the meaning of paragraph (*d*) of the definition of that expression in section 2; or

(*b*) one year in any other case.

…

24. Notwithstanding any other law, a warrant issued under section 21 or 23

(*a*) authorizes every person or person included in a class of persons to whom the warrant is directed,

(i) in the case of a warrant issued under section 21, to exercise the powers specified in the warrant for the purpose of intercepting communications of the type specified therein or obtaining information, records, documents or things of the type specified therein, or

(ii) in the case of a warrant issued under section 23, to execute the warrant; and

(*b*) authorizes any other person to assist a person who that other person believes on reasonable grounds is acting in accordance with such a warrant.

Criminal Code of Canada

183. In this Part,

"intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof;

…

"private communication" means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it;

National Defence Act

273.64 (1) The mandate of the Communications Security Establishment is

(*a*) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

(*b*) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and

(*c*) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

(2) Activities carried out under paragraphs (1)(*a*) and (*b*)

(*a*) shall not be directed at Canadians or any person in Canada; and

(*b*) shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

(3) Activities carried out under paragraph (1)(*c*) are subject to any limitations imposed by law on federal law enforcement and security agencies in the performance of their duties.

Convention on Cybercrime

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

…

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the inter-ception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

…

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Omnibus Crime Control and Safe Streets Act of 1968

2510. Definitions

…

(4) “intercept” means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.