Spies Without Borders: International Law and Intelligence Collection

Craig Forcese*

INTRODUCTION

To the surprise of many, it turns out that Canada's chief security intelligence agency – the Canadian Security Intelligence Service (CSIS) – may not legally collect covert intelligence abroad. That is at least one interpretation of a Canadian Federal Court decision issued in October 2007, but only released publicly in 2008.[1] At issue was whether the court had the jurisdiction to issue a warrant under the Canadian Security Intelligence Service Act (CSIS Act)[2] in investigations concerning Canadians taking place overseas. CSIS had sought the warrant because the targets of the investigations, as Canadians, potentially enjoyed privacy rights under Canada's constitutional bill of rights, the Canadian Charter of Rights and Freedoms.

Faced with this conundrum, there were two plausible courses of action open to the court. First, it could have concluded that the CSIS Act's warrant provisions extended only as far as authorizing searches and seizures in Canada. While this approach would have left open the question whether constitutional rules applied to CSIS's extraterritorial conduct, it would have allowed the court to avoid the incongruity of a Canadian court "legally" authorizing an invasion of privacy taking place in a foreign jurisdiction whose own laws would probably be violated by the action.

Second, the court could have reached even further and concluded that CSIS *itself* has no statutory authorization to conduct extraterritorial investigations, pursuant to its core, statutory mission to collect intelligence relating to threats to the security of Canada. This approach would avoid the constitutional question entirely, but with the consequence of greatly limiting the scope of CSIS's basic jurisdictional competence.

* Associate Professor, Faculty of Law, University of Ottawa, Canada. The author extends his thanks to the Social Science and Humanities Research Council and the Law Foundation of Ontario for their assistance over the years in financing his research. He also thanks the anonymous peer reviewer who provided careful comments on the first draft of this article.

1. *Re* Canadian Security Intelligence Service Act, 2008 F.C. 301 (Can) [hereinafter *Re* CSIS Act].

2. R.S.C., ch. C23 (1985).

Ultimately, the court chose the latter course. It took the view that Canadian statutes have no extraterritorial reach unless expressly authorized. Since, in the court's view, no such authorization can be inferred from the CSIS Act, CSIS cannot conduct security intelligence investigations overseas.

Moreover, unless expressly rebutted by the statutes themselves, Canadian statutes are to be construed in keeping with international law. The conduct of the extraterritorial investigations at issue in the case (without consent of the territorial state) would violate this international law. The CSIS investigation would involve covert electronic surveillance and, potentially, physical searches of premises in a foreign state. In the court's words: "the warrant [sought by CSIS] would therefore be authorizing activities that are inconsistent with and likely to breach the binding customary principles of territorial sovereign equality and non-intervention, by the comity of nations. These prohibitive rules of international law . . . have evolved to protect the sovereignty of nation states against interference from other states."[3]

The court's holding obviously poses a prickly policy dilemma for Canadian decisionmakers intent on collecting intelligence abroad. An obvious solution would be to modify the CSIS Act to authorize, explicitly, extraterritorial intelligence gathering. This change would cure the statutory interpretation problem raised by the court. However, legislators might be reluctant to authorize such activities if, as the court suggested, they would be in violation of international law if done without the consent of the territorial state. The court's decision raises, therefore, an important international law question that must be confronted in any reassessment of Canadian intelligence collection. More generally, the question of international law and intelligence gathering concerns all states. If the court's observations are sound, the commonplace practice of the many states that do conduct extraterritorial intelligence gathering is, by definition, illegal. The problem posed by the court's decision is, in other words, more than an idiosyncratic preoccupation for Canada. It creates implications for all states intent on squaring intelligence practices with international law.

This article addresses these implications, examining the status of peacetime spying in international law. Part I defines "spying" as the term is used in this article, focusing on collection of intelligence from human and electronic sources. The article then divides spying into geographic zones: territorial; extraterritorial; and transnational. Parts II, III, and IV then examine doctrines of international law applicable to spying in each of these three geographic areas, focusing on sovereignty rules, international immunities, and human rights principles. The article concludes that the question of international law and intelligence gathering is not easily reduced to a simple one of legality or illegality. Instead, a determination of

3. *Re* CSIS Act, *supra* note 1, at ¶52.

legality depends on a careful assessment of the location and method of the spying in question.

I. A TYPOLOGY OF SPYING

A. Defining Spying

"Spying" is a colloquial, rather than legal, term. The *Oxford English Dictionary* defines "to spy" as, among other things, "[t]o watch (a person, etc.) in a secret or stealthy manner; to keep under observation with hostile intent; to act as a spy upon" and "[t]o make stealthy observations in (a country or place) from hostile motives." Spying is often associated with "espionage" – described by the *OED* as "[t]he practice of playing the spy, or of employing spies," the latter being "a secret agent whose business it is to keep a person, place, etc., under close observation; esp. one employed by a government in order to obtain information relating to the military or naval affairs of other countries, or to collect intelligence of any kind."[4]

The image conveyed by these definitions may aptly capture one form of spying – intelligence gathered from human sources, sometimes covertly (hereafter, human intelligence). It does not, however, capture the full range of modern "intelligence gathering." "Intelligence" is the "product resulting from the collection, processing, integration, evaluation, analysis and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations."[5] Human intelligence constitutes one source of intelligence, but others exist, most notably signals intelligence.[6]

Human intelligence is often truncated to "HUMINT", a doctrinal term employed by intelligence services. For instance, the U.S. Department of the Army defines HUMINT as "the collection of information by a trained HUMINT collector . . . from people and their associated documents and media sources to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel and capabilities."[7] A "HUMINT source" may include "threat, neutral, and friendly military and civilian personnel" such as "detainees, refugees, DPs [displaced persons], local

4. OXFORD ENGLISH DICTIONARY (online version November 2010).

5. U.S. DEP'T OF DEF., DICTIONARY OF MILITARY AND ASSOCIATED TERMS 230 (as amended Sept. 30, 2010), *available at* http://www.fas.org/irp/doddir/dod/jp1_02.pdf.

6. *See* Tom Lansford, *Multinational Intelligence Cooperation*, *in* 1 COUNTERING TERRORISM AND INSURGENCY IN THE 21ST CENTURY, INTERNATIONAL PERSPECTIVES 421 (James J.F. Forest ed., 2007). There are other forms of intelligence gathering, including through remote sensing satellites, but this article concentrates on human intelligence and electronic surveillance, the most important intelligence-gathering methodologies.

7. U.S. DEP'T OF THE ARMY, HUMAN INTELLIGENCE COLLECTOR OPERATIONS, FM 2-22.3, at 1-4 (2006).

inhabitants, friendly forces, and members of foreign governmental and non-governmental organizations."[8] For the purposes of this article, human intelligence will be used in its broadest sense as "[a] category of intelligence derived from information collected and provided by human sources."[9]

Human intelligence may be provided by "assets" – that is, willing accomplices of the security service prepared to share information. It may also stem from information obtained from interrogations of persons less inclined to volunteer information. As discussed below, the legal issues raised by the recruitment of assets and the interrogation of less willing interlocutors are quite different.

For its part, signals intelligence, often reduced to SIGINT, comprises "communications intelligence and electronics intelligence."[10] In U.S. practice, "[c]ommunications intelligence consists of foreign communications passed by radio, wire, or other electromagnetic means and electronics intelligence consists of foreign electromagnetic radiations such as emissions from a radar system."[11] It is important to appreciate, however, that telecommunications interceptions may not be just foreign – domestic wiretaps are, in the broadest sense, a form of signals intelligence. However, since SIGINT is often associated with foreign intelligence intercepts, I shall use in this article the more inclusive term "electronic surveillance."

Electronic surveillance was the matter at issue in the Canadian case described above. There, the CSIS sought authorization to "intercept any telecommunication destined to or originating from the subjects of investigation . . . ."[12] To facilitate this spying, CSIS also sought permission to install, maintain and remove "any thing" required to, *inter alia*, "obtain access" to this communication[13] – presumably, a listening device of some sort. This article discusses the techniques employed for electronic surveillance; namely, equipment that can surreptitiously record actions or communications, sometimes (but not always) from great distances. In general terms, some of this surveillance may simply be the recording of behavior taking place in public spaces, such as the use of CCTV cameras. However, the fact that CSIS sought special permission by warrant to install devices suggests that this surveillance may relate to actions taking place

8. *Id.*

9. U.S. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, INTELLIGENCE COMMUNITY DIRECTIVE NUMBER 304: HUMAN INTELLIGENCE 6 (2009), *available at* www.dni.gov/electronic_reading_room/ICD_304.pdf.

10. HEARING BEFORE THE HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE, STATEMENT FOR THE RECORD OF NSA DIRECTOR LT GEN MICHAEL V. HAYDEN, USAF, at 6 n.4 (April 12, 2000), *available at* www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa24.pdf.

11. *Id.*

12. *Re* CSIS Act*, supra* note 1, at ¶14.

13. *Id.* at ¶16.

where the target may expect not to be heard by outsiders, and where surveillance of that individual requires the positioning of recording devices in intimate spaces. It may include, for example, bugging – the placement of a listening or tracking device on or around the person in places where the person might reasonably not expect to be observed – or a wiretap – the intercept of communications over phone or computer that the person might reasonably believe to be private. Put another way, surveillance may involve observing and recording conduct where a person reasonably expects privacy, raising the legal issues discussed below.

B. A Geography of Spying

Spying – whether involving human sources or electronic surveillance – has a variable geography. Neither form of intelligence gathering need be exclusively foreign or domestic. For example, while human intelligence may involve covert communications between a state agent and his or her intelligence source that take place in a foreign state, there is no requirement that this be the case. The intelligence source could, for instance, be an employee of an embassy located in the state agent's own capital. Alternatively, the communication may straddle borders, consisting of electronic or paper communications between source and agent located in different countries.

Likewise, electronic surveillance may have a domestic, foreign, and transnational nexus. As noted, a domestic wiretap may be the source of intelligence. In another scenario, one state may covertly monitor communications arising in another state from a listening facility housed in the first state's embassy in the second state's capital. In addition, signals emanating from the territory of one state may be intercepted on the territory of another.

The range of geographic permutations on spying is laid out in table 1. For the purposes of this paper, I shall use the terms "territorial" to describe purely domestic spying, "extraterritorial" to describe purely foreign spying and "transnational" to describe spying that straddles state borders.

Table 1: Geography of Spying

	Territorial	Extraterritorial	Transnational
Human intelligence	Collection of information by a state agent from people and their associated documents and media sources that takes place within the state.	Collection of information by a state agent from people and their associated documents and media sources that takes place on the territory of another the state.	Collection of information by a state agent from people and their associated documents and media sources in which the source (but not the agent) is located on the territory of another state.
Electronic surveillance	Interception of communications or actions passed by radio, wire, or other electromagnetic, photo-electronic and/or photo-optical means and of electromagnetic radiations in which both the communication and the interception takes place within the state.	Interception of communications or actions passed by radio, wire, or other electromagnetic, photo-electronic and/or photo-optical means and of electromagnetic radiations in which both the communication and the interception take place on the territory of another the state.	Interception of communications or actions passed by radio, wire, or other electromagnetic, photo-electronic and/or photo-optical means and of electromagnetic radiations in which the communication (but not the interception) takes place on the territory of another the state.

C. Spying and International Law

The international law of spying is best described as "underdeveloped," a point made repeatedly in the handful of articles on this issue.[14] As discussed below, this is particularly the case when it comes to the apparent conflict between extraterritorial spying and the sovereignty interests of the states in which the spying takes place. Ambivalence on this question does not, however, mean that spying exists in an international legal limbo. Indeed, many rules of international law may be engaged by spying, depending on the nature of that spying and its geographic location. The following sections examine the legal matters arising in relation to territorial, extraterritorial, and transnational spying.

II. TERRITORIAL SPYING

Spying conducted entirely by a state on its own territory is ultimately an area only loosely regulated by international law. The concept of state "sovereignty" lies at the core of international law, and includes, among other things, the state's "right to exercise jurisdiction over its territory and over all persons and things therein, subject to the immunities recognized by international law."[15] A state is, therefore, generally free to prescribe the forms of surveillance and investigation it wishes in relation to people, places and things on its sovereign territory.

"Generally" is, however, an important qualifier. No state now operates with unfettered sovereignty, unconstrained by other doctrines of international law. While these international obligations – to the extent they stem from treaties entered into (or not) by states – may vary between states, and some states may honor their obligations more assiduously than others,

14. *See*, *e.g.*, A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595 (2007); Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 625 (2007) (arguing that international law "has had little impact on the practice of intelligence gathering"); Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 321 (1996) (describing international law in the area as lagging behind); Daniel B. Silver (updated and revised by Frederick P. Hitz & J.E. Shreve Ariail), *Intelligence and Counterintelligence*, *in* NATIONAL SECURITY LAW 935, 965 (John Norton Moore & Robert Turner eds., 2005), (describing the status of espionage in international law as "ambiguous"); Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1091 (2004) (describing espionage as "curiously ill-defined under international law").

15. *Draft Declaration on Rights and Duties of States*, 1949 Y.B. INT'L L. COMM'N 287, art. 2. While the declaration has never been adopted, and is not in its own rights international law, it has had a "long-term effect on the development of international law"). B. Graefrath, *The International Law Commission Tomorrow: Improving Its Organization and Methods of Work*, 85, AM. J. INT'L L. 595, 595 (1991). It is fair to say that many of its provisions reflect core precepts in modern international law.

international law does provide a yardstick for criticizing (or defending) state conduct. For instance, states must abide by international human rights obligations in their conduct within their territories. As the passage cited above suggests, they must also honor immunities recognized by international law, not least diplomatic immunities. Both of these qualifiers may affect a state's domestic spying.

A. Human Rights Limitations on Spying

Both human intelligence and electronic surveillance may trigger application of international human rights norms. As noted, human intelligence, the collection of information from human assets, may involve interrogations, raising questions about the conduct of these interviews. For its part, electronic surveillance may (indeed, often does) involve surreptitious surveillance of communication or conduct, prompting issues of privacy and privacy rights.

1. Limits on Interrogation

While interrogation of uncooperative human sources may be a relatively small part of intelligence gathering as traditionally practiced, it has figured prominently in the post-9/11 debates about counterterrorism and its limits, to the point of coloring public attitudes about intelligence agencies.[16] International law guards against extreme forms of interrogation. Two broadly ratified international treaties include a prohibition on both torture and cruel, inhuman, and degrading treatment and punishment ("CID treatment"). The International Covenant on Civil and Political Rights (ICCPR) provides in Article 7 that "no one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment."[17] The Convention Against Torture and Other Cruel, Inhuman, or Degrading

16. CIA-sponsored "black sites" employed to hold and permit extreme interrogation of al Qaeda suspects provide perhaps the most recent famous example of controversy over intelligence services and their interrogation practices. In other democracies, such controversy has centered less on the interrogation practices of state security services themselves, and more on their collaboration with or facilitation of maltreatment in interrogation by allied security services in third countries. *See*, *e.g.*, COMM'N OF INQUIRY INTO THE ACTIONS OF CANADIAN OFFICIALS IN RELATION TO MAHER ARAR, REPORT OF THE EVENTS RELATING TO MAHER ARAR: ANALYSIS AND RECOMMENDATIONS (2006) (Can.); HONOURABLE FRANK IACOBUCCI, INTERNAL INQUIRY INTO THE ACTIONS OF CANADIAN OFFICIALS IN RELATION TO ABDULLAH ALMALKI, AHMED ABOU-ELMAATI AND MUAYYED NUREDDIN (2008) (Can); Patrick Wintour, Nicholas Watt & Ian Cobain, *Hague Orders Inquiry into Torture Claims*, GUARDIAN, May 21, 2010, at 2 (discussing the ongoing judicial inquiry into the role of the U.K. government in the rendition and torture of terrorist suspects).

17. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

Treatment or Punishment ("Torture Convention") includes more detailed prohibitions.[18]

a. Torture

"Torture" is defined in the Torture Convention as

> any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions.[19]

The Convention is unequivocal in outlawing torture:

> Each State Party shall take effective legislative, administrative, judicial or other measures to prevent acts of torture in any territory under its jurisdiction. . . . No exceptional circumstances whatsoever, whether a state of war or a threat of war, internal political instability or any other public emergency, may be invoked as a justification of torture. . . . An order from a superior officer or a public authority may not be invoked as a justification of torture.[20]

Moreover, "[e]ach State Party shall ensure that all acts of torture are offences under its criminal law. The same shall apply to an attempt to commit torture and to an act by any person which constitutes complicity or participation in torture."[21]

The Committee Against Torture – the treaty body established by the Torture Convention – has rejected efforts to justify torture on national security grounds, such as counterterrorism.[22] Meanwhile, under the ICCPR,

18. Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, S. Treaty No. Doc. 100-20 (1988), 1465 U.N.T.S. 85 [hereinafter Torture Convention].

19. *Id.* at art. 1.

20. *Id.* at art. 2.

21. *Id.* at art. 4.

22. *See*, *e.g.*, Comm. Against Torture, *Conclusions and Recommendations of the Committee Against Torture*, at ¶4, U.N. Doc. CAT/C/CR/29/4 (Dec. 23, 2002) ("The Committee is aware of the difficulties that the State party faces in its prolonged fight against

freedom from torture and CID treatment are among the rights for which no derogation is permitted, even in times of emergency that threaten the life of the nation.[23]

b. Cruel, Inhuman, and Degrading Treatment

As noted, the ICCPR bars CID treatment. The Torture Convention also specifies:

> Each State Party shall undertake to prevent in any territory under its jurisdiction other acts of cruel, inhuman or degrading treatment or punishment which do not amount to torture as defined in article 1, when such acts are committed by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity.[24]

CID treatment is not defined in either the Torture Convention or the ICCPR. It is commonly viewed as egregious treatment that falls short of outright torture.[25] No clear standard determines, however, how egregious this conduct must be to constitute CID treatment. The U.N. General Assembly has urged that the term be "interpreted so as to extend the widest possible protection against abuses, whether physical or mental."[26] However, the Human Rights Committee established by the ICCPR has declined to "draw up a list of prohibited acts or to establish sharp distinctions between the different kinds of punishment or treatment [barred by Article 7 of the ICCPR]; the distinctions depend on the nature, purpose and severity of the treatment applied."[27] It has further observed that "what

terrorism, but recalls that no exceptional circumstances whatsoever can be invoked as a justification for torture . . . .").

23. ICCPR, *supra* note 17, at art. 2.

24. Torture Convention, *supra* note 18, at art. 16.

25. *See*, *e.g.*, Declaration on the Protection of All Persons from Being Subjected to Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, G.A. Res. 3452, Annex, 30 U.N. GAOR, Supp. No. 34, 91, art. 1, U.N. Doc. A/10034 (1975) ("Torture constitutes an aggravated and deliberate form of cruel, inhuman or degrading treatment or punishment."); 2 RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES, §702, Reporters' Notes, No. 5, at 170 (1987) (citing Ireland v. United Kingdom, 25 Eur. Ct. H.R. ser. A., ¶167 (1978) for the proposition that "[t]he difference between torture and cruel, inhuman, or degrading treatment or punishment 'derives principally from a difference in the intensity of the suffering inflicted'"). *See also* Mehinovic v. Vuckovic, 198 F. Supp. 2d 1322, 1348 (N.D. Ga. 2002) ("Generally, cruel, inhuman, or degrading treatment includes acts which inflict mental or physical suffering, anguish, humiliation, fear and debasement, which do not rise to the level of 'torture' or do not have the same purposes as 'torture.'").

26. Code of Conduct for Law Enforcement Officials, *adopted by* G.A. Res. 34/169, art. 5, Commentary (c) (Dec. 17, 1979).

27. Human Rights Comm., General Comment No. 20, Article 7, ¶4 U.N. Doc. HRI\GEN\1\Rev.1 (1994).

constitutes inhuman or degrading treatment falling within the meaning of Article 7 depends on all the circumstances of the case, such as the duration and manner of the treatment, its physical or mental effects as well as the sex, age and state of health of the victim."[28]

In at least one instance, the Human Rights Committee has accepted that the rationale for the treatment may be relevant in determining its legal character. In a case against Australia, it held that a state's legitimate fear of the flight risk posed by prisoners warranted the shackling of those individuals and rendered this act something other than CID treatment.[29] The Committee has been reluctant, however, to take this line of reasoning too far. It appears, therefore, to reject state justifications for certain forms of treatment, including corporal punishment,[30] a state action the Committee readily declares to be CID treatment.[31] It has also indicated that where an act does, in fact, constitute CID treatment, no justification exonerates the injuring state. As noted, there is to be no derogation from Article 7 even in a time of national emergencies, presumably the most potent public interest motivation imaginable.[32]

Despite an unwillingness to define *ex ante* the exact contours of the CID treatment standard, both the Human Rights Committee and the Committee Against Torture have identified specific state practices they view as constituting CID treatment.

---

28. Human Rights Comm., Commc'n. No. 265/87 (Vuolanne v. Fin.), 249, U.N. Doc. Supp. No. 40 (A/44/40) (1989), *available at* .http://www1.umn.edu/humanrts/undocs/session44/265-1987.htm

29. Human Rights Comm.,Commc'n. No. 1020/01 (Bertran v. Austl.), ¶8.2, U.N. Doc CCPR/C/78/D/1020/2001 (2003), *available* at http://www1.umn.edu/humanrts/undocs/1020-2001.html.

30. Human Rights Comm., Comm*c'n*. No. 759/97 (Osbourne v. Jam.), ¶9.1, U.N. Doc. CCPR/C/68D/759/1997 (2000), *available at* http://www1.umn.edu/humanrts/undocs/session68/view759.htm ("Irrespective of the nature of the crime that is to be punished, however brutal it may be, it is the firm opinion of the Committee that corporal punishment constitutes cruel, inhuman and degrading treatment or punishment contrary to article 7 of the Covenant").

31. Human Rights Comm., General Comment No. 20, Article 7, *supra* note 27, at ¶5.

32. *Id.* at ¶3 ("The text of article 7 allows of no limitation. The Committee also reaffirms that, even in situations of public emergency such as those referred to in article 4 of the Covenant, no derogation from the provision of article 7 is allowed and its provisions must remain in force. The Committee likewise observes that no justification or extenuating circumstances may be invoked to excuse a violation of article 7 for any reasons, including those based on an order from a superior officer or public authority."). *See also* J. HERMAN BURGERS & HANS DANELIUS, THE UNITED NATIONS CONVENTION AGAINST TORTURE 150 (1988) ("Unlike in the definition of torture . . . the purpose of the act is irrelevant in determining whether or not the act should be considered to constitute cruel, inhuman or degrading treatment. . . ."); SARAH JOSEPH, JENNY SCHULTZ & MELISSA CASTAN, THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS: CASES, MATERIALS AND COMMENTARY 212 (2004).

For instance, the particular acts declared CID treatment by the Committee Against Torture include:

> substandard detention facilities lacking basic amenities such as water, electricity and heating in cold temperatures;[33]
>
> long periods of pre-trial detention and delays in judicial procedure coupled with incarceration in facilities ill equipped for prolonged detention;[34]
>
> beating prisoners who are also denied medical treatment and are deprived of food and proper places of detention;[35]
>
> virtual isolation of detainees for a period of a year;[36]
>
> use of electro-shock belts and restraint chairs as means of constraint;[37]
>
> acts of police brutality that may lead to serious injury or death;[38] and,
>
> deliberate torching of houses.[39]

Commenting specifically on interrogation techniques, the Committee Against Torture has also identified the following as CID treatment: "(1) restraining in very painful conditions, (2) hooding under special conditions, (3) sounding of loud music for prolonged periods, (4) sleep deprivation for prolonged periods, (5) threats, including death threats, (6) violent shaking, and (7) using cold air to chill."[40] This list is roughly analogous to similar lists of techniques found to be inhuman and degrading by the European

33. Comm. Against Torture, Report of the Committee Against Torture, ¶183, U.N. Doc. A/56/44 (2001).

34. *Id.* at ¶119.

35. Comm. Against Torture, Report of the Committee Against Torture, ¶175, U.N. Doc. A/53/44 (1998).

36. Comm. Against Torture, Report of the Committee Against Torture, ¶¶58, 61, U.N. Doc. A/55/44 (2001).

37. *Id.* at ¶¶179, 180.

38. Comm. Against Torture, *supra* note 33, at ¶64.

39. Comm. Against Torture, Commc'n No. 161/00 (Dzemajl v. Yugo.), U.N. Doc. CAT/C/@(/D/161/2000 (2002), *available at* http://www1.umn.edu/humanrts/cat/decisions/161-2000.html.

40. Comm. Against Torture, *Concluding Observations of the Committee Against Torture: Israel,* ¶257, U.N. Doc. A/52/44 (1997), *available at* http://www.unhchr.ch/tbs/doc.nsf/%28Symbol%29/A.52.44,paras.253-260.En?OpenDocument.

Court of Human Rights under the European Convention on Human Rights[41] and improper by the Israeli Supreme Court.[42]

Specific acts identified by the Human Rights Committee as constituting CID treatment do not differ greatly from those invoked by the Committee Against Torture. They include abduction of an individual followed by detention without contact with family members;[43] denial of food and water;[44] denial of medical assistance after ill-treatment;[45] death threats;[46] mock executions;[47] whipping and corporal punishment;[48] failure to notify a family of the fate of an executed prisoner;[49] prolonged detention on death row when coupled with "further compelling circumstances relating to the detention. . .";[50] and detention in substandard facilities[51] or conditions.[52]

41. Ireland v. United Kingdom, 23 Eur. Ct. H.R. (ser. B) (1976), at 3 (discussing protracted standing on the tip of the toes; covering of the head for the duration of the detention; exposure to loud noise for a prolonged period, and deprivation of sleep, food and water).

42. HCJ 5100/94 *Public Committee Against Torture in Israel v. Israel*, ¶29 (1999) (Isr.) (declaring improper the "Shabach" method, composed of several components: the cuffing of the suspect, seating him on a low chair, covering his head with a sack, and playing loud music in the area).

43. Human Rights Comm. Commc'n No. 542/1993 (Tshishimbi v. Zaire*)*, ¶5.5, U.N. Doc. CCPR/C/53/D/542/1993 (1996), *available at* http://www1.umn.edu/humanrts/undocs/html/542-1993.html; Human Rights Comm. *Commc'n No*. 540/1993 (*Atachahua v. Peru)*, ¶8.5, U.N. Doc. CCPR/C/56/D/540/1993 (1993), *available at* http://www1.umn.edu/humanrts/undocs/540-1993.html.

44. Human Rights Comm., Commc'n No. 414/1990 (Miha v. Equatorial Guinea*),* ¶6.4, U.N. Doc. CCPR/C/51/D/414/1990 (1994), *available at* http://www1.umn.edu/humanrts/undocs/html/vws414.htm.

45. *Id. See also*, Human Rights Comm., *Commc'n No*. 334/1988 *(*Bailey v. Jam.*)*, ¶9.3, U.N. Doc. CCPR/C/47/D/334/1988 (1993), *available at* http://www1.umn.edu/humanrts/undocs/html/334-1988.html.

46. Human Rights Comm., Commc'n No. 407/1990 (Hylton v. Jam.*)*, ¶9.3, U.N. Doc CCPR/C/57/D/600/1994 (1994), *available at* http://www1.umn.edu/humanrts/undocs/html/VWS60057.htm.

47. Human Rights Comm., Commc'n No. 255/1987 (Linton v. Jam.*)*, ¶8.5, U.N. Doc. CCPR/C/46/D/255/1987 (1992), *available at* http://www1.umn.edu/humanrts/undocs/html/dec255.htm.

48. Human Rights Comm., Commc'n No. 792/1998 (Higginson v. Jam.), ¶4.6, U.N. Doc. CCPR/C/74/D/792/1998 (2002)*, available at* http://www.unhcr.org/refworld/country.HRC,,JAM,,3f588ef33,0.html; Human Rights Comm., *Commc'n No*. 928/2000 (*Sooklal v. Trinidad and Tobago)*, at ¶4.6, U.N. Doc. CCPR/C/73/D/928/2000 (2001), *available at* http://www1.umn.edu/humanrts/undocs/928-2000.html.

49. Human Rights Comm., Commc'n No. 886/1999 (Schedko v. Belarus*)*, ¶10.2, U.N. Doc. CCPR/C/77/D/886/1999 (2003), *available at* http://www1.umn.edu/humanrts/undocs/886-1999.html.

50. Human Rights Comm., Commc'n No. 553/1993 (Bickaroo v. Trin & Tobago*)*, at ¶5.6, U.N. Doc. CCPR/C/61/D/555/1993 (1997), *available at* http://www1.umn.edu/humanrts/undocs/session61/vws555.htm.

51. Human Rights Comm., Commc'n No. *607/1994* (Adams v. Jam.), ¶¶3.15, 8.2, U.N. Doc. CCPR/C/58/D/607/1994 607/1994 (1996), *available at* http://www.1umn.

Examples of CID treatment stemming from the conditions of detention include:

> incarceration for fifty hours in an overcrowded facility, resulting in prisoners being soiled with excrement, coupled with denial of food and water for a day;[53]
>
> incarceration in circumstances falling below the standards set in the U.N. Standard Minimum Rules for the Treatment of Prisoners, coupled with detention *incommunicado*, death and torture threats, deprivation of food and water and denial of recreational relief;[54]
>
> solitary incarceration for ten years in a tiny cell, with minimal recreational opportunities;[55]
>
> solitary incarceration *incommunicado* for various periods;[56] and,
>
> incarceration with limited recreational opportunities, no mattress or bedding, no adequate sanitation, ventilation or electric lighting, and denial of exercise, medical treatment, nutrition and clean drinking water.[57]

c. Humane Treatment of Detainees

Detention in the circumstances described above may also run afoul of Article 10 of the ICCPR, guaranteeing that states treat persons deprived of their liberty with humanity and dignity. The Human Rights Committee has concluded that Article 10 rights attach to "anyone deprived of liberty under

edu/humanrts/undocs/html/VWS607.htm.

52. Human Rights Comm., Commc'n No. 619/1995 (Deidrick v. Jam.) ¶9.3, U.N. Doc. CCPR/C/62/D/619/1995 (1998), *available at* http://www1.umn.edu/humanrts/undocs/html/VWS607.htm.

53. Human Rights Comm., Commc'n No. 188/1984 (Protorreal v. Dom. Rep.), at ¶¶9.2, 11, U.N. Doc. CCPR/C/OP/2 at 214 (1990), *available at* http://www1.umn.edu/humanrts/undocs/newscans/188-1984.html.

54. Human Rights Comm., Commc'n No. 458/1991 (Mukong v. Cameroon), ¶¶9.3, 9.4, U.N. Doc. CCPR/C/51/D/458/1991 (1994), *available at* http://www1.umn.edu/humanrts/undocs/html/vws458.htm.

55. Human Rights Comm., Commc'n No. *529/1993* (Edwards v. Jam.), ¶8.3, U.N. Doc. ccpr/c/60/d/529/1993 (1993), *available at* http://www1.umn.edu/humanrts/undocs/529-1993.html.

56. Human Rights Comm., Commc'n No. *577/1994* (Campos v. Peru), ¶8.6, U.N. Doc. CCPR/C/61/D/577/1994 (1997), *available at* http://www.bayefsky.com/docs.php/area/jurisprudence/treaty/ccpr/opt/0/node/4/filename/108_peruvws577 (detention incommunicado for one year); Shaw v. Jam, U.N. Human Rights Committee File 704/1996 ¶7.1 (June 4, 1998) (detention incommunicado for 8 months in overcrowded and damp conditions).

57. Human Rights Comm., Commc'n No. *775/1997* (Brown v. Jam.). ¶6.13, U.N. Doc. CCPR/C/65/D/775/1997 (1999), *available at* http://www.bayefsky.com/docs.php/area/jurisprudence/treaty/ccpr/opt/0/node/4/filename/255_jamaica002.

the laws and authority of the State," including those who are held in prisons or "detention camps."[58]

Article 10 has been interpreted as prohibiting acts less severe than outright CID treatment, particularly where a person has been detained in generally poor conditions but has not been singled out for particularly egregious treatment.[59] The committee has also found violations of Article 10 when detainees are held *incommunicado* for periods of time shorter than those declared CID in other cases.[60]

Compliance with the U.N. Standard Minimum Rules for the Treatment of Prisoners[61] may also be relevant in determining whether a state complies with Article 10.[62] These rules establish detailed standards in such areas as hygiene, food, clothing and bedding, exercise and sport, medical services, discipline and punishment, and contact with the outside world.

2. Limits on Surveillance

Covert electronic surveillance indisputably impairs privacy. Privacy rights are entrenched in international human rights law, most notably in the ICCPR. They are, however, not absolute – indeed, the protection they offer is muted, making them a limited constraint on state electronic surveillance so long as certain basic protections are observed. As Charles Garraway argues, "[t]argeted interference with the right to privacy in accordance with domestic law would not seem to run afoul of the human rights provision of itself, although the targeting will need to be carefully designated so that it does not violate the prohibition against discrimination" found in Article 2 of the ICCPR.[63]

58. Human Rights Comm., General Comment No. 21, Article 10, 33, ¶2, U.N. Doc. HRI/GEN/1/Rev.1 (1994).

59. Human Rights Comm., *Commc'n No. 493/1992 (*Griffin v. Spain*)*, at ¶6.3, U.N. Doc. CCPR/C/53/D/493/1992 (1995), *available at* http://www1.umn.edu/humanrts/undocs/html/vws493.htm (concluding that art. 10 applied in relation to generally poor conditions of incarceration, even where art. 7 CID treatment was not established); *see also* JOSEPH, SCHULTZ & CASTAN, *supra* note 32, at 277.

60. Human Rights Comm., *Commc'n No. 147/1983 (*Gilboa v. Uruguay*)*, 176, ¶14, U.N. Doc. CCPR/C/OP/2 (1990), *available at* http://www1.umn.edu/humanrts/undocs/newscans/147-1983.html (incommunicado detention for fifteen days a violation of Article 10).

61. Adopted by the First United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held at Geneva in 1955, and approved by the Economic and Social Council by its resolution 663 C (XXIV) of 31 July 1957 and 2076 (LXII) of 13 May 1977.

62. *See* Human Rights Comm., General Comment No. 21, Article 10, *supra* note 58, at ¶5.

63. Charles H.B. Garraway, *State Intelligence Gathering: Conflicts of Laws*, 28 MICH. J. INT'L L. 575, 581 (2007).

The core privacy right is found as Article 17 of the ICCPR: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. . . . Everyone has the right to the protection of the law against such interference or attacks."[64] The concept of "privacy" is not well defined in the ICCPR – it does not prescribe, for example, a concept of zones in which a reasonable expectation of privacy might exist. That said, the invocation of "home" and "correspondence" suggests that these, at the very least, are zones given special protection against interference.

In relation to this interference, it is notable that the U.N. Human Rights Committee has reiterated that Article 17 protects against "unlawful" and "arbitrary" intrusion, with unlawful meaning that "no interference can take place except in cases envisaged by the law" and that the law must itself "comply with the provisions, aims and objectives of the Covenant."[65] The concept of "arbitrariness", for its part, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances."[66]

The Committee further specifies:

> Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.[67]

It has since opined, in a complaint brought under the ICCPR's first optional protocol, that state searches of a home, "without legal grounds," constitute an arbitrary interference with privacy, family, and home within the meaning of Article 17.[68]

The Committee is also obviously prepared to conflate the "correspondence" invoked in Article 17 with more general forms of communication:

> Correspondence should be delivered to the addressee without interception and without being opened or otherwise read.

64. ICCPR, *supra* note 17, at art. 17.

65. Human Rights Comm., General Comment No. 16, Article 21, ¶3, U.N. Doc. HRI/GEN/1/Rev.1 (1994).

66. *Id.* at ¶4.

67. *Id.* at ¶8.

68. Human Rights Comm., Commc'n No. 1460/2006 (Yklymova v. Turkmenistan*)*, at ¶7.6, U.N. Doc. CCPR/C/96/D/1460/2006 (2009), *available at* http://www.bayefsky.com/docs.php/area/jurisprudence/treaty/ccpr/opt/0/state/177/node/4/filename/turkmenistan_t5_iccpr_1460_2006.

> Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.[69]

"Home", meanwhile, includes not only the domicile, but also the place of usual occupation.[70]

The Committee's views are not international law themselves, but can properly be considered instructive in construing the otherwise ambiguous reach of Article 17.[71] From these views, it stands to reason that communications generally as well as actions that take place in the home or place of work are protected by the ICCPR's rules on interference by the state, whether by virtue of being a subset of the (undefined) international concept of "privacy" or, instead, as a part of "home" or "correspondence."

International "soft-law" standards also exist. Notable among these are the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[72] These guidelines provide that "[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject."[73] This person should be notified of the use to which this information will be put, and any subsequent disclosure of this information should be consistent with this use.[74] Exceptions to these principles are permissible for reasons of, among other things, national security, but should be as few as possible and be made known to the public.[75] The U. N. General Assembly has also proposed guidelines with similar provisions.[76]

3. Discussion

In sum, international human rights law contains several provisions that relate to intelligence collection, even within a state's own territory. These provisions do not address spying per se, instead being broadly crafted

69. Human Rights Committee, General Comment No. 16, *supra* note 65, at ¶8.

70. *Id.* at ¶5.

71. *See* DOMINIC MCGOLDRICK, THE HUMAN RIGHTS COMMITTEE: ITS ROLE IN THE DEVELOPMENT OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (1991).

72. Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, Sept. 23, 1980, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2.

73. *Id.* at Principle 7.

74. *Id.* at Principles 9-10.

75. *Id.* at Principle 4.

76. U.N. General Assembly, Dec. 14, 1990, Guidelines for the Regulation of Computerized Personal Data Files, U.N. Doc. A/RES/45/95.

norms that have the effect of regulating how spying can be conducted. Put simply, the norms are: 1) human intelligence cannot be extracted through abusive interrogation, and 2) electronic surveillance of communications or surveillance that amounts to intrusions into the "home" (including the place of work) must be authorized by law and by the appropriate official, on a case-by-case basis, and be reasonable in the circumstances.

B. Limitations on Spying Stemming from International Immunities

A second area of public international law affecting a state's territorial spying relates to international immunities, and in particular those enjoyed by diplomats. A state's jurisdiction over accredited diplomats is greatly constrained in public international law. First, the person of the diplomat is "inviolable," in the sense that he or she is not "liable to any form of arrest or detention" and the receiving state must treat him or her "with due respect" and "take all appropriate steps to prevent any attack" on his or her "person, freedom or dignity."[77] The diplomat is also immune from the criminal jurisdiction of the receiving state.[78]

More importantly from an intelligence-gathering perspective, the diplomatic premises are themselves inviolable. The Vienna Convention on Diplomatic Relations provides that "[t]he premises of the mission shall be inviolable. The agents of the receiving State may not enter them, except with the consent of the head of the mission."[79] Further, "[t]he receiving State is under a special duty to take all appropriate steps to protect the premises of the mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity" and "[t]he premises of the mission, their furnishings and other property thereon and the means of transport of the mission shall be immune from search, requisition, attachment or execution."[80] Meanwhile, "[t]he archives and documents of the mission shall be inviolable at any time and wherever they may be"[81] and "[t]he official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions."[82] Nor may the diplomatic bag "be opened or detained."[83] Analogous protections extend to the personal premises of diplomats, and to their papers and correspondence.[84]

77. Vienna Convention on Diplomatic Relations, Apr. 18, 1961, 500 U.N.T.S. 95, art. 29.

78. *Id.* at art. 31.

79. *Id.* at art. 22.

80. *Id.*

81. *Id.* at art. 24.

82. *Id.* at art. 27.

83. *Id.*

84. *Id.* at art. 30.

As a consequence, states that intercept communications occurring in diplomatic missions or the personal premises of diplomats violate international law. Likewise, a state that opens official diplomatic correspondence acts unlawfully, although the caveat that "[o]fficial correspondence means all correspondence relating to the mission and its functions" may open the door to interception of foreign state correspondence unrelated to the mission and its functions.[85] Of course, since a diplomat will hardly signal that a given communication falls into one category or another, intercepting an inappropriate communication falling outside diplomatic functions necessarily would require the interception of appropriate diplomatic communication as well. Put another way, the caveat could swallow the immunity, if applied aggressively.

The question of whether a state could spy on diplomats operating on its territory was a live controversy in the United States at the time of the enactment of the Foreign Intelligence Surveillance Act (FISA) in 1978. Congress reportedly expressed unease that electronic surveillance directed at diplomatic premises would violate the Convention. The Administration overcame this concern by supplying a list of states that surveilled U.S. diplomatic premises abroad, suggesting that such a widely accepted practice, while not authorized by the Convention, did not violate it.[86] It is, however, difficult to see how spying on diplomats, even if widespread, can be squared with the actual rules found in the Convention, unless one accepts the doubtful proposition that interception of communications is permitted in an effort to separate official correspondence from correspondence not properly related to the mission's functions. Thus, while spying on diplomats may be commonplace, it is no less a violation of the Convention.

III. EXTRATERRITORIAL SPYING

States do not confine their spying to their own territory, instead also collecting intelligence from the territories of other states. Extraterritorial spying raises supplemental international law issues, most notably the potential clash between state sovereignty and spying. Also relevant are questions concerning the extraterritorial reach of the human rights principles discussed above.

85. *See* Note, *Who's Listening: Proposals for Amending the Foreign Intelligence Surveillance Act*, 70 VA. L. REV. 297, 319 n.97 (1984).

86. Jeffrey H. Smith, Symposium, *State Intelligence Gathering and International Law: Keynote Address*, 28 MICH. J. INT'L L. 543, 545 (2007).

A. State Sovereignty Limitations on Extraterritorial Spying

As noted, sovereignty is a core precept of public international law, guarding a state's essentially exclusive jurisdiction over its own territory. A concomitant principle is that "[e]very State has the duty to refrain from intervention in the internal or external affairs of any other State" and "the duty to refrain from fomenting civil strife in the territory of another State, and to prevent the organization within its territory of activities calculated to foment such civil strife."[87]

The principle of non-interference in sovereign affairs is recognized most famously in the U.N. Charter itself, which provides in Article 2(4) that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." The principle is, however, broader than this preoccupation with use of force suggests. As the influential General Assembly Declaration on Principles of International Law concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations declares, "[e]very State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State" and "[n]o State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State."[88] While not itself a source of public international law, the Declaration is almost certainly a reflection of current customary international law.[89]

There are undoubted examples of espionage – broadly defined to include, e.g., covert military assistance – that exceed the non-interference standard. U.S. support to the *contras* in Nicaragua in the 1980s constitutes the most notable example of such an instance available in the international jurisprudence.[90] A more difficult issue is whether the spying, as this article uses the term, transgresses the non-interference rules. Here, there are possible gradations of legality.

1. Spying in Aid of Use of Force

First, espionage conducted as preparation for an armed attack may be considered a "threat or use of force" precluded by the U.N. Charter and customary international law. It is, therefore, a violation of international law

87. *Draft Declaration on Rights and Duties of States, supra* note 15, at arts. 3, 4.

88. G.A. Res. 2625 (XXV), Annex, U.N. GAOR, 25th Sess., Supp. No. 28, at 123, U.N. Doc. A/5217 (Oct. 20, 1970).

89. *See*, *e.g.*, *Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14, ¶202.

90. *Id. See also* Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 MICH. J. INT'L L. 687, 691-692 (2007).

unless the use of force at issue is itself authorized by the Security Council under chapter VII of the U.N. Charter or is lawful as an exercise of self-defense.[91]

This last caveat may be an important one in practice. Some scholars argue that "the surreptitious collection of intelligence in the territory of other nations that present clear, articulable threats based on their past behavior, capabilities, and expressions of intent, may be justified as a practice essential to the right of self-defense."[92] Plausible examples of the latter may include spying in response to the proliferation of weapons of mass destruction and state-sponsored terrorism.[93] This assertion is difficult to square with the doctrinal law of self-defense. It is not clear how spying in aid of self-defense is permissible where the right to self-defense is not yet triggered as a matter of international law by, among other things, a sufficiently imminent armed attack. Nevertheless, some scholars envisage a more forgiving standard for spying in self-defense, urging that spying even before there is evidence of such an imminent attack is necessary for states to prevent or protect against armed attacks if the right to self-defense is to remain meaningful.[94]

2. Spying by Diplomats

Passive collection of open source intelligence information (from, for example, public sources or the diplomatic community) by accredited diplomats is permissible. The Vienna Convention on Diplomatic Relations provides that diplomats have a duty not to interfere in the internal affairs of the receiving state and that diplomatic mission premises must not be "used in any manner incompatible with the functions of the mission as laid down in the present Convention or by other rules of general international law or by any special agreements in force between the sending and the receiving State."[95]

However, the precise functions of a diplomatic mission consist, among other things, of "[a]scertaining by all *lawful means* conditions and developments in the receiving State, and reporting thereon to the Government of the sending State."[96] According to the International Law Commission commentaries on the draft articles that became the Convention, the phrase "conditions and developments" "covers the

91. For a discussion of spying in support of a right to self-defense, see Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F.L. REV. 217, 223 (1999).

92. *Id.* at 225.

93. *Id.*

94. *See* Baker, *supra* note 14, at 1096.

95. Vienna Convention on Diplomatic Relations, *supra* note 77, at art. 41.

96. *Id.* at art. 3 (emphasis added).

political, cultural, social and economic activities of the country, and in general all aspects of life which may be of interest to the sending State."[97]

Much hinges on the "lawful means" caveat on the collection of information by diplomats. A state might expressly preclude such information collection by law, thereby rendering all such activities unlawful. It is difficult to see, however, how such a law – squeezing the full function of ascertaining conditions and developments into the "unlawful" category – could be squared with the Convention. Such a law would use the "lawful means" exception to negate the very function anticipated by the treaty. Nor is it clear that this approach could be reconciled with the Convention's guarantee of diplomatic "free communications" for all "official purposes" and "freedom of movement and travel in its territory," except in those zones regulated for reasons of national security.[98]

More difficult to categorize is the active collection of intelligence from human or electronic sources. Using a diplomatic mission as an electronic communications listening post might easily be an unlawful activity prohibited by the Convention – such a post may intercept, for example, cell phone communications that, within the state's own laws applied even to its own law enforcement, cannot be intercepted without warrants. Breaking into a residence to plant a listening device certainly falls outside the scope of "lawful means" of information collection in any state with a reasonable set of laws. Likewise, communication with a human asset in a sensitive security sector may induce a breach of official secrets laws applicable to that asset.

In sum, spying by diplomats may be constrained by international law, not because of an express prohibition on such activity but because the type of spying in question falls outside the limits of the diplomatic function. It is notable, however, that even then, international law does not impose express punishment on diplomats. When a diplomat's espionage activities trigger a reaction by the receiving state, that person is (merely) declared *persona non grata*, the response permitted by the Convention to malfeasance by diplomats. However, while the receiving state "typically says [the diplomat's] activities were inconsistent with diplomatic activities," it is

97. 1958 Y.B. INT'L L. COMM'N, Vol. II, at 90, U.N. Doc. A/CN.4/117.

98. Vienna Convention on Diplomatic Relations, *supra* note 77, at arts. 26, 27. Security zones are not just the product of repressive states. Even democracies manage entry into sensitive areas, including military bases, and criminalize surveillance of these places. For instance, in Canada, "[e]very person commits an offence who, for any purpose prejudicial to the safety or interests of the State, approaches, inspects, passes over, is in the neighborhood of or enters a prohibited place at the direction of, for the benefit of or in association with a foreign entity or a terrorist group." Security of Information Act, R.S.C. 1985, c. O-5, s. 6 (Can.). A "prohibited place" includes military facilities, but also any place designated by the government "to be a prohibited place on the ground that information with respect thereto or damage thereto would be useful to a foreign power." *Id.* at s. 2.

reportedly rare for the state to claim that these activities themselves violate international law.[99] Nor have there been instances where states have invoked the optional protocol to the Convention,[100] which provides that disputes concerning the interpretation or application of the Convention's provisions on espionage may be brought before the International Court of Justice (ICJ). The ICJ came closest to opining on peacetime espionage in the Teheran Hostages case, where it noted the difficulty in determining when a diplomat's function of "ascertaining by all lawful means conditions and developments in the receiving State" constitutes espionage or interference in internal affairs. This lack of precision is, however, overcome by permitting states to declare diplomats *persona non grata* entirely at their discretion.[101] There is, in other words, no need for precise definition of proper diplomatic functions where states retain the discretion to, in essence, define these functions according to their own standards.

In the view of at least some academic commentators, the failure of states to allege international illegality in condemning spying supports an argument that extraterritorial spying is legal as a matter of customary international law, a point explored in greater detail in the following section.

3. Spying by Other State Agents

For their part, non-diplomatic state agents collecting human intelligence or engaging in electronic surveillance do not benefit from any diplomatic cover, or arguments that their activities fall within the scope of a diplomatic mission. They are, therefore, personally culpable for any violation of the laws of the state in which they spy, and their states are responsible for any resulting breaches of international law. In this last respect, everything hinges on the breadth of the customary prohibition on intervening "directly or indirectly, for any reason whatever, in the internal or external affairs of any other State." Does, for instance, a failure by a state agent to comply fully with the territorial state's laws always amount to a breach of the latter's sovereignty and of international law?

The exercise of what is known as "enforcement jurisdiction" by one state and its agents in the territory of another is clearly a breach of international law – it is impermissible for one state to exercise its power on the territory of another, absent consent or some other permissive rule of international law.[102] More uncertain is whether a state agent's violation of

99. Smith, *supra* note 86, at 544.

100. Optional Protocol Concerning the Compulsory Settlement of Disputes, Vienna, Italy, Apr. 18, 1961, 500 U.N.T.S. 241.

101. Case Concerning United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, 40 (May 24).

102. The Case of the S.S. Lotus (Fr. v. Tur.), 1927 P.C.I.J. ser. A No. 10, at 18 (Sept. 7)

domestic security rules by spying necessarily constitutes a violation of international law.

In times of armed conflict, spies are harshly punished – they are not, for instance, entitled to prisoner of war status in an international conflict. On the other hand, a spy's government "is not violating law in sending him, and his act is not, therefore, a war crime."[103] Espionage in times of armed conflict is legitimate because of the "absence of any general obligation of belligerents to respect the territory or government of the enemy state"[104] – after all, sovereignty is not a concept that dovetails with use of armed force.

The situation in peacetime is different. There is no international jurisprudence on peacetime espionage conducted by one state's agents in the territory of another, and the academic literature is deeply divided on the question of legality. Writing in 1962, Quincy Wright noted that "very little has been said about" peacetime espionage in the international law literature.[105] However, he urged that "espionage and, in fact, any penetration of the territory of a state by agents of another state in violation of the local law, is also a violation of the rules of international law imposing a duty upon states to respect the territorial integrity and political independence of other states . . . It belongs to each state to define peacetime espionage . . . as it sees fit, and it is the duty of other states to respect such exercise of domestic jurisdiction."[106] It follows that "any act by an agent of one state committed in another state's territory, contrary to the laws of the latter, constitutes intervention, provided those laws are not contrary to the state's international obligations."[107]

Wright urges that it is no defense to the claim that espionage is unlawful in international law to argue that it is commonplace. While this may be true, the surreptitious nature of espionage and the general unwillingness of states to acknowledge that they practice it, or allege it in instances where spies are discovered, is "accompanied not by a sense of right but by a sense of wrong."[108] Even if it is commonplace, spying is a poor candidate for a customary international law exception to sovereignty – whatever state practice exists in the area is hardly accompanied by *opinio juris*. Simon Chesterman echoes Wright on this point in his 2006 article,

("the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State"), *available at* http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm.

103. Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 11 (Roland Stanger ed., 1962).

104. *Id.* at 12. For an additional discussion of espionage and spying in the law of armed conflict, see Demarest, *supra* note 14.

105. Wright, *supra* note 103, at 10.

106. *Id.* at 12, 13.

107. *Id.* at 13.

108. *Id.* at 17.

noting the disconnect between the widespread practice of state spying and a state propensity to, at the same time, condemn spying directed at it.[109] In these circumstances, Chesterman suggests that state practice and *opinio juris* run in opposite directions. Put another way, there is little doctrinal support for a "customary" defense of peacetime espionage in international law.

For his part, Manuel Garcia-Mora, writing in 1964, regards peacetime spying as illegal, arguing that "peacetime espionage is regarded as an international delinquency and a violation of international law," but acknowledging that this matter is heatedly disputed.[110] This position is also shared by Ingrid Delupis, in a 1984 article on foreign warships and espionage.[111]

Other international lawyers demur on this question, to varying degrees. Lassa Oppenheim, commenting in passing on the question in 1920, noted that while spies are punished severely when caught, peacetime spying "is not considered wrong morally, politically or legally."[112] Writing in 1973, Myres McDougal, Harold Lasswell, and Michael Reisman argued that the "number of formal protests [sparked by spying] which have been lodged have been relatively insignificant. This latter practice suggests a somewhat ambivalent perspective upon the part of national elites in regard of such activities and may indicate a deep but reluctant admission of the lawfulness of such intelligence gathering, when conducted with customary normative limits."[113] These authors note that while each state penalizes espionage in its domestic laws, "no systematic attempt has been made to assimilate the activity to *delicta juris gentium*"[114] – that is, make it an international crime. In his more recent article, Demarest appears to share this view, concluding that "[w]hile clandestine information gathering will continue to be considered an unfriendly act between nations, such activity does not violate international law."[115]

In his own assessment of the question, Roger Scott observed in 1999 that "the status of espionage under international law remains ambiguous,

109. Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1072 (2006).

110. Manuel R. Garcia-Mora, *Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition*, 26 U. PITT. L. REV. 65, 79-80 (1964).

111. Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 Am. J. INT'L L. 53, 67 (1984).

112. LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE, at §455 (Ronald F. Roxburgh ed., 1920).

113. Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, *The Intelligence Function and World Public Order*, 46 TEMPLE L. Q. 365, 394 (1973).

114. *Id.*

115. Demarest, *supra* note 14, at 347.

not specifically permitted or prohibited."[116] No international convention prohibits that practice "because all states have an interest in conducting such activity."[117] On the other hand, "it is doubtful that espionage in another nation's territory will ever be explicitly acknowledged as 'legal' under the law of nations" because of its transgression of a state's territorial sovereignty.[118] In essence, the regulation of foreign espionage is a matter left to the laws and diplomatic practices of individual states, producing uneven responses to the phenomena.

Christopher Baker shares Scott's view on the ambivalence of international law to espionage, noting in his 2004 article the absence of either affirmative endorsements or rejections of espionage in international treaties and describing the status of espionage in international law as "curiously ill-defined."[119] For his part, Daniel Silver argues that addressing the legality of espionage in international law is almost "oxymoronic" given the universal propensity of states to both spy on others and condemn spying directed at them. Like other authors, he notes that espionage is not specifically prohibited by treaty or other forms of international law, but describes spying as also "not formally tolerated under customary international law except in wartime, where the activity is regarded as accepted practice governed by the laws of war."[120]

Jeffrey Smith, writing in 2007, is prepared to go further, arguing that "because espionage is such a fixture in international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law."[121] Likewise, Glenn Sulmasy and John Yoo urge that "[s]tate practice throughout history . . . supports the legitimacy of spying. Nowhere in international law is peaceful espionage prohibited. Domestic law punishes captured spies not because they violate some universal norm against espionage, but because they have engaged in intelligence operations against national interests."[122]

Reviewing most of these authorities, John Radsan subdivides the academic literature into three categories: those who regard espionage as illegal in international law; those who see it as "not illegal;" and those who envisage espionage as neither legal nor illegal.[123] The very fact that there are three camps with such diametric positions itself suggests that the third position lies closest to the truth: there is no clear answer on the international

116. Scott, *supra* note 91, at 223.
117. *Id.* at 220.
118. *Id.* at 223.
119. Baker, *supra* note 14, at 1094.
120. Silver, *supra* note 14, at 965.
121. Smith, *supra* note 86, at 544.
122. Sulmasy & Yoo, *supra* note 14, at 628.
123. Radsan, *supra* note 14, at 595.

legality of extraterritorial espionage, assessed from the sovereignty perspective, and the international community seems content with an artful ambiguity on the question.

B. Human Rights Limitations on Extraterritorial Spying

As discussed in Part A of this article, human rights principles constrain the means and methods of spying within a state's own borders by prohibiting torture, cruel, inhuman, and degrading treatment, and unauthorized intrusions into privacy. At issue in this section is whether those same principles affect a state's extraterritorial intelligence collection activities. The answer to this question depends on whether international human rights instruments have extraterritorial reach.

1. The Extraterritorial Reach of the Torture Convention

A focus on territoriality runs through the Torture Convention. Article 16 of the Torture Convention, prohibiting cruel, inhuman, and degrading treatment, obliges states to take efforts to prevent CID treatment "in any territory under its jurisdiction." This phrase is also repeated in the Torture Convention's Article 2, describing the obligation of states to take all legal steps to stop torture "in any territory under its jurisdiction." This language evolved during the course of the treaty's drafting. The original draft of the Torture Convention employed a simple reference to "under its jurisdiction" in Article 2. France voiced concern, however, that the latter phrase was too sweeping, and would oblige a state to regulate the conduct of its citizens residing in another state. The inclusion of "in any territory" would instead confine the Article 2 obligation to the territorial bounds of a state, ships and aircraft registered to a state, and to any occupied territory.[124]

This view prevailed. Subsequently, publicists have interpreted the repeated references in the Convention to "in any territory under its jurisdiction" as capturing a state's "land territory, its territorial sea and the airspace over its land and sea territory", as well as territories under military occupation, colonial territories, and "any other territories over which a State has factual control."[125]

2. The Extraterritorial Reach of the ICCPR

The geographic reach of the ICCPR is likely broader than that of the Torture Convention. Whether the ICCPR provisions prohibiting torture,

124. *See* BURGERS & DANELIUS, *supra* note 32, at 48.

125. *Id.* at 131, 149 (discussing Article 5 and extending the Article 5 observations to Article 16).

cruel, inhuman, and degrading treatment, and unauthorized intrusions into privacy reach a state's extraterritorial conduct depends on the interpretation of Article 2 of the Torture Convention. Article 2 describes the scope of a state's overall ICCPR obligations as follows: "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant." An important issue is, therefore, whether individuals subject to the extraterritorial intelligence collection are within the "territory and subject to [the state's] jurisdiction."

Article 2 talks about territory *and* jurisdiction, implying that the two concepts are alternative descriptions of the ICCPR's reach. This possibility is accommodated by international law, which clearly views jurisdiction and territory as separate concepts. For instance, states may exercise prescriptive jurisdiction in relation to their nationals irrespective of their location.[126]

In practice, both the Human Rights Committee and the International Court of Justice have concluded that individuals may be within a state's jurisdiction, even while not on its territory. In the original Human Rights Committee case in which this doctrine was first pronounced, the victim was kidnapped, abused, and secreted out of the country by Uruguayan security agents operating in Argentina.[127] The Human Rights Committee considered that the victim was nevertheless within the jurisdiction of Uruguay.

More recently, the Human Rights Committee and the International Court of Justice have concluded that a person may be within a state's jurisdiction when that person is within the power or "effective control" of the state, even if not on the state's territory.[128] Whether detention for the purposes of interrogation constitutes sufficient "effective control" may

126. *See* 1 RESTATEMENT (THIRD) THE FOREIGN RELATIONS LAW OF THE UNITED STATES, §402 (1987) (generally, "a state has jurisdiction to prescribe law with respect to . . . the activities, interests, status, or relations of its nationals outside as well as within its territory").

127. Human Rights Comm., Commc'n No. 52/1979 (Lopez v. Uru.), U. N. Doc. CCPR/C/13/D/52/1979 (1984), *available at* http://www1.umn.edu/humanrts/undocs/html/52_1979.htm.

128. Human Rights Comm., General. Comment 31, ¶10, U.N. Doc. A/59/40 (2004) (observing that "a State party must respect and ensure the rights laid down in the Covenant to anyone within *the power or effective control* of that State Party, *even if not situated within the territory* of the State Party" (emphasis added). In its review of state reports on compliance with the ICCPR, the committee has also suggested that state obligations extend to a state's armed forces stationed abroad. *See*, *e.g.*, Human Rights Comm., Concluding observations of the Human Rights Comm.: Neth., ¶8, U.N. Doc. CCPR/CO/72/NET (2001) (relating to the "alleged involvement of members of the [Netherlands] State party's peacekeeping forces in the events surrounding the fall of Srebrenica, Bosnia and Herzegovina, in July 1995. . ."). More recently, the International Court of Justice referred to this committee jurisprudence in *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*. In that advisory opinion, it concluded that a state's ICCPR obligations had extraterritorial reach: "the Court considers that the International Covenant on Civil and Political Rights is applicable in respect of acts done by a State in the exercise of its jurisdiction outside its own territory." Advisory Opinion, 2004 I.C.J. 136, ¶111 (July 9).

depend on the particulars of individual cases. However, it is notable that the highest court in the United Kingdom, interpreting equivalent obligations under the European Convention on Human Rights, recently held that events occurring within a British detention center in Iraq were within the United Kingdom's jurisdiction for the purposes of the treaty.[129]

3. Discussion

In sum, a state's obligations under the Torture Convention extend to territories over which it has factual control, while its ICCPR responsibilities attach to persons under its effective control, including, potentially, those detained surreptitiously for purposes of interrogation. The rules governing extreme forms of interrogation do, therefore, extend to extraterritorial intelligence collection from human sources.

It is difficult to see, however, how the ICCPR concept of "effective control" applies to the privacy interests protected by Article 17 or constrains, for instance, extraterritorial electronic surveillance. Extraterritorial surveillance almost by definition will not be of persons within the spying state's effective control. The surveilled individual is, therefore, neither within the surveilling state's "territory" or "jurisdiction" and the ICCPR privacy protections are inapplicable.

IV. TRANSNATIONAL SPYING

Transnational spying is obviously the most geographically complex form of intelligence gathering. Recall that transnational spying arises where the source of the intelligence, but not the recipient, is located in a foreign state.

Electronic surveillance in particular is a likely method of transnational spying, given that signals originating in state A may, depending on the technology involved, be intercepted on the territory of state B. Perhaps the most famous form of transnational SIGINT foreign intelligence collection involves a consortium of "Anglo-sphere" states – the United States, the United Kingdom, Australia, Canada, and New Zealand. These states collaborate in signals intelligence, pursuant to the confidential U.K.-U.S. security agreement dating in its original form to 1947.[130] This collaboration – well publicized as the so-called ECHELON network – drew scrutiny from the European Parliament in 2001, which described it as a "global system for

129. Al-Skeini v. Sec'y of State for Def., [2007] UKHL 26 (U.K.).

130. COMMUNICATIONS SECURITY ESTABLISHMENT, CANADA'S MOST SECRET INTELLIGENCE AGENCY, BP-343E (1993), *available at* http://dsp-psd.tpsgc.gc.ca/Collection-R/LoPBdP/BP/bp343-e.htm.

intercepting communications."[131] Human intelligence may also, however, be "transnational," by virtue of forms of communication that allow a source in state A to communicate with a state agent in state B.

From an international legal perspective, there is little about transnational spying that distinguishes it from purely extraterritorial spying. Human rights obligations are tied to the location of the person whose rights are at issue – in consequence, the rules governing the extraterritorial reach of international human rights instruments do not differ when the spying is transnational and not purely extraterritorial. Likewise, the state from whose territory the intelligence originates may raise sovereignty objectives tied to interference in its internal affairs, even if that interference is directed from the spying state's own territory.

There are some circumstances, however, where transnational intelligence gathering may be treated differently than purely extraterritorial actions: some transnational intelligence gathering may be simply passive, in the sense that an electronic signal originating in one state is captured in another. It is difficult to see how the interception of electronic leakage from one state from the territory of another state violates a sovereignty interest. It is true that in respect to this sort of intelligence collection at least one additional legal instrument relating to transnational telecommunications may be relevant: the International Telecommunications Convention provides that members will "take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence."[132] This is, however, hardly a resounding prohibition, as the treaty also states that members "[n]evertheless, . . . reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their internal laws or the execution of international conventions to which they are parties."[133] Put another way, a domestic law steering international communications to a security agency on national security grounds is plausibly an "internal law" that trumps the secrecy proviso found in the Convention.

Of potentially greater relevance are provisions of the Vienna Convention on Diplomatic Relations that require states to accord official correspondence and communications transmitted through their state from a diplomatic premise in a third state "the same freedom and protection as is accorded by the receiving State" – that is, the state in which the diplomat is

131. EUROPEAN PARLIAMENT, REPORT ON THE EXISTENCE OF A GLOBAL SYSTEM FOR THE INTERCEPTION OF PRIVATE AND COMMERCIAL COMMUNICATIONS (ECHELON INTERCEPTION SYSTEM) 133 (July 11, 2001), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN.

132. International Telecommunication Convention, Nov. 6, 1982, art. 22, 1531 U.N.T.S. 319 (entered into force Jan. 1, 1984).

133. *Id.*

working.[134] The rules governing the inviolability of diplomatic communication cannot, in other words, be circumvented by transnational electronic surveillance of diplomats accredited to third party states.

CONCLUSION

Public international law rules pertaining to spying are best described as a checkerboard of principles, constraining some practices in some places and in relation to some actors, but not in other cases in relation to other actors. There is no simple rule, in other words, governing the international legality of spying. Table 2 reproduces the core conclusions of this article, divided by international legal rule and geographic zone.

Table 2: International Law and Spying

	Territorial	Extraterritorial	Transnational
Human rights limitations on interrogation via torture or CID treatment	Apply	Apply, where the victim is within the effective control of the state	Do not apply, as by definition victim not within effective control of the state
Human rights limitations on interception of private communications	Apply	Do not apply, because the victim is not within the effective control of the state	Do not apply, because the victim is not within the effective control of the state
Diplomatic immunities	Apply, limiting the ability of the receiving state to spy on foreign diplomats	Apply, permitting information collection by foreign diplomats so long as done by "lawful means"	Apply, limiting the ability of states to intercept transiting communications from diplomats accredited to third party states
Sovereignty limitations on interference in internal affairs	Non-applicable	Apply, but international law is very uncertain as to whether peacetime spying is impermissible	Apply, but international law is very uncertain as to whether peacetime spying is impermissible

134. Vienna Convention on Diplomatic Relations, *supra* note 77, at art. 40.

The most yawning gap in the coverage of international law in the area of peacetime espionage is in its ambivalent approach to extraterritorial spying and the sovereignty rule. It is exactly this preoccupation with sovereignty that animated the Canadian Federal Court decision with which this article began. As noted, that court was unequivocal in considering spying without the consent of the territorial state a violation of international law. This article suggests that international law is, in fact, less precise on this question, and indeed that views on this matter differ dramatically.

This observation prompts a final point. While compliance with international law may rank far down the list of concerns some intelligence agencies face in conducting their activities, a revealed failure to comply is, at the very least, embarrassing, and in some countries a potential source of scandal. It is also a potential legal disability in states, such as Canada, that increasingly look to international law in construing domestic constitutional or other obligations, including obligations in their intelligence-gathering operations. Here, the policy of creative ambivalence that has characterized state attitudes towards spying and international law may prove costly. The Canadian Federal Court decision is illustrative. In that case, CSIS sought to square what it perceived to be its domestic constitutional obligations with its international practices. In so doing, it asked a court to authorize conduct that, from first principles, gave every appearance of violating core precepts of the sovereignty norm, in circumstances where international scholars themselves debate the exact state of the law. The court acted reasonably in erring on the side of caution and refusing to give judicial blessing to conduct that, if revealed, would create thorny problems in international relations.

As noted, it will be no simple thing to overcome this caution by legislative amendment. No Canadian politician, cognizant of Canada's modest position in the hierarchy of nations, will enthusiastically endorse an amendment that authorizes emphatically what other states only accept tacitly – that extraterritorial spying is permissible.

In the result, CSIS has a choice: conduct extraterritorial spying without recourse to the courts, at risk of ultimately being called to account under domestic law, or honor the Canadian Federal Court's construal of international law (and CSIS's jurisdiction) and pull in its truly international surveillance operations, potentially blinding the country's chief security intelligence agency.[135] This is not a happy situation, and it is a consequence at some level of a failure by the international community to extend a legal imprimatur to the reality of international spying.

135. It is notable that in a subsequent case, CSIS made sure that its communication intercepts, while of international communications, occurred physically within the territory of Canada – here there was no infringement of the territorial sovereignty of a third state. Asked to authorize a warrant in these circumstances, the Federal Court pointed to this domestic territorial nexus in approving the warrant and distinguishing this matter from that at issue in the earlier case discussed in the text above. *Re* Canadian Security Intelligence Service Act, 2009 F.C. 1058 (Can).