AN ASSESSMENT OF THE LEGAL REGIME GOVERNING THE FINANCING OF TERRORIST ACTIVITIES IN CANADA

By

Anita Indira Anand*

* Anita Indira Anand, B.A., B.A., LL.B., LL.M., Associate Professor, Faculty of Law, University of Toronto. Opinions expressed are those of the author, and do not necessarily represent those of the Commission or the Commissioner. Thanks to Kent Roach for helpful comments and to Karen Andreychuk and Amy Murakami for valuable research assistance. Thanks to Patricia Marson for her assistance in preparing the document.

TABLE OF CONTENTS

1. INTRODUCTION

This study analyzes Canada's legal approach to combating the financing of terrorist activities. It also undertakes a comparative discussion with U.S. law to isolate cross-country differences in legislative and procedural mechanisms designed to prevent terrorist financing. Underlying the legal discussion is an analysis of the role of, and costs imposed upon, the private sector in monitoring and reporting financial transactions; the balance between privacy rights and deterring the financing of terrorism; and, the need to assess the efficacy of particular legal instruments in combating the financing of terrorism.

Although anti-terrorist financing law did not exist in 1985 when Air India Flight 182 was bombed, today's legal regime appears to be comprehensive. It is based primarily on two pieces of legislation examined here: first, the Criminal Code, and, second, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. These legislative initiatives cover significant regulatory ground in terms of substantive law, and, generally speaking, they also accord with private and public international law on terrorist financing.[1] The difficulty with the contemporary regime lies not in conspicuous gaps in the substantive law, but rather in knowing whether the regime is effective in fulfilling its stated objectives of preventing and disrupting the funding of terrorists.

This study focuses on the need to assess the current anti-terrorist financing regime and ensure that its infrastructure functions effectively. First, it suggests that a formal and full-fledged assessment of the efficacy of the current regime be undertaken. Second, it suggests that consideration be accorded as to whether a body that oversees and monitors the functions of FINTRAC should be created. Third, in the same vein, it suggests that study be undertaken on the issue of whether a larger oversight body is necessary, one that oversees not only the activities of FINTRAC, but also other institutions that bear responsibility for enforcing the terrorist financing laws, such as the RCMP and CSIS.

Thus, this study takes a pragmatic view of law. Law generally, and anti-terrorist financing law specifically, should not be viewed as a panacea

---

1 The one area where this may not be true is in the area of reporting suspicious attempted transactions. However, the recommendations in Bill C-25 largely address this shortcoming. See Bill C-25, *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a Consequential Amendment to Another Act*, 1st Sess., 39th Parl., 2006, section 3(1)(g) [*Bill C-25*]. Bill C-25 received Royal Assent on December 14th and became S.C. 2006, c.12.

that can cure all political evils. Law is a tool, and, at times, a limited one. Unless we know whether current law is effective, we should not be keen to create additional legal requirements. This is because regulation is costly, and ineffective regulation imposes unnecessary costs.

Part 2 of this paper outlines the elements of the Canadian legal regime aimed at combating the financing of terrorist activities. Part 3 examines, on a comparative basis, the U.S. legal system regarding this subject to evaluate whether the Canadian regime is missing any important structural or legal elements. Part 4 contains the analysis central to this report including directions for future consideration and research. Part 5 concludes the discussion.

2. CANADIAN REGIME

The Canadian regime to counter the financing of terrorist activities has two main component parts: first, the amendments to the Criminal Code of Canada that deal with terrorist financing[2] and other related provisions in the Criminal Code[3], and, second, Proceeds of Crime (Money Laundering) and Terrorist Act.[4] As these legal instruments were implemented within the past six years, they are ripe for evaluation, especially in light of claims that Canada is a "haven" for terrorists.[5] This section will examine these two layers of regulation.[6]

At the outset, it bears mentioning that Canada's regime relating to the financing of terrorism appears to accord with international obligations. For example, Canada is a founding member of the Financial Action Task Force (FATF), an intergovernmental body of 33 countries that includes terrorist financing in its mandate. FATF has passed eight special recommendations on terrorist financing that have become international standards and that have provided a blueprint for the domestic law of its members. In addition, Resolution 1373 adopted by the UN Security Council in 2001

---

2 R.S.C. 1985, c. C-46, sections 83.01-83.27 **[***Criminal Code***].**

3 See *e.g.*, *ibid*., sections 462.32(4), 462.35 relating to the seizing of property and time periods under which property can be detained.

4 S.C. 2000, c. 17 [*Proceeds of Crime Act* or *the Act*].

5 U.S. Library of Congress, *Asian Organized Crime and Terrorist Activity in Canada*, (Washington, D.C.: Library of Congress 2003). See also "U.S. again brands Canada terrorist haven", *The Globe and Mail* (15 February 2004).

6 It should be noted that there are other aspects of the regulatory regime dealing with terrorism, as distinct from the financing of terrorism. These are usefully described in the recent Arar Inquiry Report. See Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, (Ottawa: Ministry of Public Works, 2006) c. 3 [*Arar Inquiry Report*].

states that countries shall "deny safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe havens…"[7] It further states that countries shall "prevent those who finance, plan, facilitate, or commit terrorist acts from using their respective territories for those purposes…"[8] The Security Council Resolution does not provide guidance on structures that need to be established in order to effect these objectives. Nevertheless, as discussed here, Canada has abided by the Resolution in terms of the laws it has passed.

Implicit in this analysis is an understanding that terrorism, and the financing of terrorism, defies geographical boundaries.[9] A prime example is that money can be transferred without actually changing hands (for example, *via* an exchange of debt system).[10] Thus, an analysis of Canada's laws is necessarily of limited use as questions persist regarding the extra territorial application of these laws. Two issues outside the mandate of this paper are significant here: whether the legislation at issue should be read to have extraterritorial effect; and, whether private and public international law permits Canada to apply its law to conduct in question.[11] Notably, however, the recent Criminal Code amendments discussed below may entail expanded jurisdiction to try offences committed outside of Canada if such offences would fall within the provisions of the Code.[12]

Criminal Code

Section 83.01(1)(a)(x) of the Criminal Code defines "terrorist activities" as including acts committed outside or inside Canada that if committed in Canada would constitute an offence under section 83.02 in relation to providing or collecting property intending or knowing that it will be used for terrorism.[13] The list of what actions constitute a "terrorist activity" is lengthy, and includes conspiracy, attempt, or threat to commit listed acts

---

7 *Charter of the United Nations*, SC Res. 1373(2001), UN SCOR, 2001,UN Doc. S/RES/1373 (2001), section 2(c).

8 *Ibid*., section 2(d).

9 Walter Perkel, "Money Laundering and Terrorism: Informal Value Transfer Systems" (2003) 41 Am. Crim. L. Rev. 183-184.

10 *Ibid.* at 188-189.

11 *Supra* note 9 at 194-195 discussing extra-territoriality of U.S. law.

12 See Criminal Code, *supra* note 2, section 7 (3.73) (extending jurisdiction to prosecute s,.83.02 offence committed outside of Canada in certain circumstances). See *supra* note 2, section 7 (3.74) (extending jurisdiction to prosecute other terrorism offences committed outside of Canada in certain circumstances).

13 *Ibid.,* section 83.01(x) referring to subsection 7(3.73) that implemented *the International Convention for the Suppression of the Financing of Terrorism*, adopted by the General Assembly of the United Nations on December 9, 1999.

or omissions.[14] The first set of criminal offences is contained in sections 83.02-83.04, and consists of a three-pronged approach to counter terrorist financing. The offences are all indictable offences under which the accused is liable to imprisonment for a term of not more than ten years if convicted.

Specifically, section 83.02 of the Criminal Code imposes prohibitions on providing or collecting property to carry out terrorist activity. The provision applies to everyone who directly or indirectly "willfully and without lawful justification or excuse provides or collects property intending that it be used or knowing that it will be used" to carry out a terrorist activity has committed an offence under the Code. Although the prohibited act of this offence is defined quite broadly to the direct or indirect provision or collection of property, the offence has high fault requirements that require proof of an intent or knowledge that the property will be used for terrorism.

Section 83.03 creates an offence for anyone who directly or indirectly collects property, provides, or makes available property for terrorist purposes. The Code provides that no person shall knowingly deal in property that is owned or controlled by a terrorist group, or facilitate directly or indirectly any transaction in respect of such property. The prohibited act of this offence is also defined very broadly, and section 83.03(b) is quite broad because it applies to anyone who provides, or even invites a person to provide, property or financial or other related services knowing that will be used in whole or part to benefit a terrorist group. It is not necessary under section 83.03(b) to demonstrate any connection with any terrorist activity: "it is an offence merely to 'use' or 'possess' property with the intention or knowledge that it will be used for terrorist purposes".[15]

Section 83.04 creates an offence for using or possessing property for terrorist purposes. In particular, anyone who "uses property, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist activity" has violated the statute. Similarly, if a person possesses property and intends that it will be used, or knows that it will be used, to facilitate terrorist activity, they have violated the statute. This offence is

---

14 *Ibid.*

15 Kevin E. Davis, "The Financial War on Terrorism" in Victor V. Ramraj, Michael Hor, and Kent Roach, eds. *Global Anti-Terrorism Law and Policy* (Cambridge: Cambridge University Press, 2005) 182.

again worded broadly, but requires proof that the accused either has the purpose of facilitating or carrying out a terrorist activity, or intends or knows that it will be used for such purposes. The fault requirements of these various offences would have to be proven beyond a reasonable doubt.

In addition, under section 83.05(1), the Governor in Council may establish a list of entities that have knowingly carried out, facilitated, or attempted to carry out terrorist activities, or knowingly acted on behalf of terrorist entities. Once an entity is a listed entity, it will fall within the definition of "terrorist group" in section 83.01. A terrorist group is not, however, restricted to those entities, forty at present, that have been listed under section 83.05, and includes an entity that has as one of its purposes the facilitation or carrying out of terrorist activities, including an association of such entities.

A second set of offences relates to freezing and forfeiture of property. Under section 83.08, no person in Canada, or a Canadian outside of Canada, is permitted to deal with property knowing that it is controlled by a terrorist group, or provide financial or other related services for the benefit of a terrorist group. Furthermore, under section 83.1(1), every person in Canada, and every Canadian outside of Canada, must disclose to the RCMP and CSIS "the existence of property in their possession or control that they know is owned or controlled by, or on behalf of, a terrorist group", as well as information about a transaction or proposed transaction in respect of such property.

Under section 83.11(1), certain listed financial institutions must determine on a continuing basis whether they are in possession or control of such property, and must make reports regarding the same on a monthly basis. Anyone who contravenes these offences is liable, on summary conviction, to a fine of $100,000, or imprisonment for one year maximum, or both, or, if convicted on indictment, to imprisonment for a maximum of ten years. Unlike the offences under section 83.02-83.04, these offences are aimed primarily not at terrorists and their supporters, but to third parties who might deal with terrorist property. Such third parties may be more amenable to regulation; but, as discussed below, care should be taken not to impose unreasonable and costly burdens on them. Furthermore, section 83.09 contains an exemption scheme which allows the Solicitor General to provide an exemption from liability arising under one of the several provisions that prohibit the financing of terrorists.

In addition to these sections of the Criminal Code that deal specifically with financing of terrorism, Part XII.2 Proceeds of Crime addresses money laundering. If someone deals with property, or any proceeds of property, with the intent to conceal the property, and knowing or believing that all or part of the property was obtained from the commission or omission of a designated offence, she is liable to be convicted on either indictable offence or summary conviction.[16] Case law decided under the section suggests that past prosecutions have not involved terrorist activities per se, but to such things as drug trafficking[17] and, of course, money laundering alone.[18] Terrorism can be financed not only by money derived from crime, but also by money derived from other sources, including legitimate earnings, and funds given to charities.

The money laundering provisions are extremely broad and deal with "property or proceeds obtained directly or indirectly". Strictly interpreted, these provisions contain a broad *actus reus*. The New Brunswick Court of Appeal has held (affirming a decision at first instance) that in order for property to be included as proceeds of crime, the property must be directly linked to the commission of the criminal act in question.[19] Establishing the *mens rea* requirement is also potentially problematic, since the accused must "know or believe all or some [of the property or proceeds] was obtained directly or indirectly…" Again, this is an extremely broad phrase, and suggests that "almost any connection with criminal activity will be caught by this section".[20]

As will be noted below, there is some overlap between the obligations in the Criminal Code and those contained in the Proceeds of Crime Act which raises the question of whether this area of law is "overregulated". First, they both contain provisions that aim to address money laundering. Second, they both contain reporting requirements. The Criminal Code requires that every person in Canada, and every Canadian outside of Canada, disclose information about a transaction, or proposed transaction, in respect of property owned or controlled by, or on behalf of, a terrorist group. Similarly, the Proceeds of Crime Act contains reporting requirements that apply to a list of entities that closely resembles the list contained in the Criminal Code. Third, they both have provisions relating

---

16 Criminal Code, *supra* note 2, sections 462.31(1), 462.31(2).
17 See *e.g. Giles v. Canada* [1991] 63 C.C.C. (3d) 184.
18 *R. v.Hape* [2000] 148 C.C.C. (3d) 530.
19 *R. v. Shalala* (1998), 198 N.B.R. (2d) 298, aff'd [2000] N.B.R. (2d) 118. See also David Samuel-Strausz Vernon, "A Partnership with Evil: Money Laundering, Terrorist Financing and Canadian Financial Institutions" (2004) 20 B.F.L.R. 89 at 94.
20 Laundering Database (May 1, 1998) at para 8 online www.quicklaw.com.

to the compilation of a list of terrorist entities; and they both seek to target entities that "facilitate" the financing of terrorist activities.

While overlap between criminal and regulatory offences is common, one of the functional problems of overlap is the existence of different, and possibly uncoordinated, enforcement regimes. In particular, prosecution of terrorist offences under the Criminal Code must be pre-approved by the provincial or federal Attorney General. But, who enforces the Proceeds of Crime reporting requirements (FINTRAC and/or police authorities); and, is there a need for co-ordination between the enforcement authorities?

Proceeds of Crime Act

While the Criminal Code addresses a variety of activities that relate to terrorist financing (from providing property, to assist in terrorist financing, to money laundering) and criminalizes such activity, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act deals with reporting requirements, cross-border movement of currency, and the creation of an agency to administer the Act.

Under section 7 of the Act, defined individuals and entities report transactions "in respect of which there are reasonable grounds to suspect that the transaction is related to the commission of…a terrorist activity financing offence."[21] In addition, if these individuals and entities are required to make a report under section 83.1 of the Criminal Code, they must also make the report to the agency that is responsible for administering the Proceeds of Crime Act: the Financial Transactions and Reports Analysis Centre (FINTRAC).[22] FINTRAC's purpose is to facilitate the detection, prevention, and deterrence of money laundering and the financing of terrorist activities. FINTRAC also has the authority to receive voluntary information from various sectors of the public, including law enforcement agencies, about suspicions of terrorist financing. [23]

The fact that reports must go to FINTRAC and, under the Criminal Code, to the heads of the RCMP and CSIS, suggests that the legislation creates a system, perhaps for privacy reasons, in which agencies do not share information. While information sharing may be beneficial for efficiency and

---

21 *Proceeds of Crime Act*, *supra* note 4, section 7.
22 *Ibid.,* section 7.1(1).
23 *Ibid.,* section *7*.1.

efficacy reasons, Posner has argued that post-9/11, the U.S. government chose reforms that result in a top-heavy and overly centralized intelligence system. Posner argues that in intelligence generally, it is best to have multiple centers, as centralization can be ineffective.[24] This is a point that will be discussed further below.

Every person or entity that breaches the reporting requirements contained in the Act is liable on summary conviction to a $500,000 fine or 6 months in prison or both for first time offences. For subsequent offences, the fine is increased to $1,000,000 and the prison term is one year or both; or, on conviction on indictment, to a $2,000,000 fine or 5 years in prison or both. Thus, for failing to report, persons or entities face significant penalties. It is not clear on the face of the statute which body enforces contravention of the Act when these offences occur.

The Act contains a defence for employees in respect of transactions that they reported to their superiors.[25] However, directors and officers are guilty of an offence if they direct, authorize, assent to, acquiesce in, or participate in an act that violates the statute.[26] These individuals do have a defence available if they establish that they exercised due diligence to prevent the commission of the act.[27] However, the liability of directors and officers under the statute appears to be a regulatory offence.

In addition to the reporting requirement on individuals and entities, persons arriving in or leaving Canada must file reports regarding the importation and exportation of currency or monetary instruments over a prescribed amount.[28] Customs officers may retain currency and monetary instruments at the border, and these are forfeited to the federal government.[29] Officers may search these individuals,[30] conveyances,[31] and baggage,[32] as well as any mail being imported or exported.[33]

Under the Act, the persons and entities that have reporting and monitoring functions to FINTRAC under section 7 include: authorized

---

24 Richard A. Posner, *Uncertain Shield : The U.S. Intelligence System in the Throes of Reform* (Lanham: Rowman & Littlefield, 2006).
25 *Proceeds of Crime Act*, *supra* note 5, section 75(1).
26 *supra note 5*
27 *Ibid.,* section 79(b).
28 *Ibid.,* section 12(1), 12(3).
29 *Ibid*., section 14(5).
30 *Ibid*., section 15(1).
31 *Ibid*., section 16(1).
32 *Ibid*., section 16(2).
33 *Ibid*., section 17(1).

banks, cooperative credit societies, loan and trust companies, portfolio managers, securities dealers, casinos, and various other business entities. [34] Amendments to the Act contained in Bill C-25 broaden the persons and entities required to engage in record-keeping and reporting of activities; this list now includes businesses that deal in securities or any other financial instruments, for example.[35] However, even with these amendments, there are undoubtedly organizations and less formal institutions (such as "hawals", informal trust-based systems for transferring funds[36]) that are not subject to reporting obligations under the statutory schema. Simply because the breadth of the list has been expanded under Bill C-25 does not mean that such organizations will be caught by its terms.

Bill C-25 also attempts to deal with the issue of funds channeled through charitable organizations. The Bill amends the Income Tax Act to allow the Canada Revenue Agency (CRA) to disclose to FINTRAC, the RCMP, or CSIS information about charities suspected of being involved in terrorist financing activities.[37] It appears from the legislation that the CRA is able to choose the entity to which it provides information.[38] The Bill C-25 amendments to the Income Tax Act also permit information sharing among CSIS and the RCMP for purposes of investigating whether an offence may have been committed, or whether certain activities constitute securities threats. But there is no requirement for information sharing, and certainly no oversight body that monitors the conduct of these organizations when they act pursuant to the legislation.

Common law has established that there is a duty of secrecy and confidentiality on bankers in their relationships with customers. In *Tournier v National Provincial & Union Bank of England*, the English Court of Appeal held that the bank is the custodian of its customers' confidential information and has a duty not to disclose such information.[39] However, the case also isolated certain exceptions to the rule, including where there is a duty to the public to disclose, or where the interests of the bank require disclosure. Thus, it could certainly be argued on either of these grounds that where a terrorist organization is utilizing a bank for the funneling of illegal funds contrary to the law of Canada, it is in the public

---

34 *Ibid*., section 5.
35 *Bill C-25, supra* note 1.
36 U.S., National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, D.C.: United States Government Printing Office, 2004) at 171.
37 *supra note 2*
38 *Ibid*.
39 (1923), [1924] 1 K.B. 461 (C.A.).

interest, as well as the bank's own interest, to disclose these transactions.[40] Furthermore, there are certain legislative provisions that protect banks and others from civil claims.[41]

The proposed amendments in Bill C-25 also broaden the scope of the reporting obligation. Whereas the current Act requires reporting of every financial transaction that *occurs* and is related to the commission of a terrorist activity financing offence, the amendments deal with "every financial transaction that occurs or that is *attempted*…and in respect of which there are reasonable grounds to suspect that:…(b) the transaction is related to the commission *or the attempted commission* of a terrorist activity financing offence."[42] In addition, the Bill adds a new prohibition to the Act which prohibits persons from opening an account on behalf of the person if it cannot establish his or her identity.[43] These persons must also determine whether they are dealing with a "politically exposed foreign person"[44] and, if so, they must obtain the approval of senior management before proceeding.[45] Numerous measures must be adopted before an entity enters into a banking relationship with a foreign entity.[46]

FINTRAC is in many senses a gatekeeper of information. It receives information from three bodies: federal agencies such as CSIS and the RCMP, foreign intelligence bodies and, of course, reports regarding suspicious transactions from the private sector.[47] FINTRAC also makes decisions regarding where to channel this information, if anywhere. If it has reasonable grounds to suspect that designated information would be relevant to investigating or prosecuting terrorist activity, FINTRAC must disclose the information to the appropriate police force, Revenue Canada, and the Canada Border Services Agency.[48] It is required to

---

40 However, it should be noted first that such a breach of confidentiality is likely in advance of any hard proof that the laws of Canada have been broken. Thus, it would not be clear if the public interest were indubitably at risk. Furthermore, laws that compel disclosure of customers' information run the risk of invading their privacy, an issue discussed in greater detail below.

41 See Criminal Code, *supra* note 3, section 83.1(2) which states that "No criminal or civil proceedings lie against a person for disclosure made in good faith under subsection (1)".

42 supra note 3

43 supra note 2

44 This term is defined as a "person who holds or has held one of the following offices or positions in or on behalf of a foreign state", and includes a list consisting of a number of officials including: head of state or head of government, deputy minister, ambassador, head of government agency, judge… See *Bill C-25, supra* note 2, section 8.

45 supra note 2

46 *Ibid.*

47 See *Arar Inquiry Report*, *supra* note 7 at 567.

48 *supra note 7*

disclose information to CSIS if it "has reasonable grounds to suspect that designated information would be relevant to threats to the security of Canada".[49]

The term "designated information" means, in respect of a financial transaction, the name of the client, the name and address of the place where the transaction occurred, the amount and type of currency involved, the transaction number and the account number, and any other identifying information that may be prescribed.[50] FINTRAC may also disclose designated information to an institution or agency of another country or an international organization.[51] However, FINTRAC may not disclose any information that would serve to identify an individual who provided information to it[52], and cannot disclose information provided to it in regards of suspicious transactions. FINTRAC is required, however, to disclose information if it determines that there are reasonable grounds to suspect that the information would be relevant to investigating a terrorist financing or money laundering offence.[53]

Not contained in the legislative schema is a list of the criteria to be applied by FINTRAC in making a decision regarding whether to provide information to CSIS and/or the RCMP. However, FINTRAC's 2006 Annual Report states:

> Once we determine that there are reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering and/or terrorist activity financing offence and/or threats to the security of Canada, FINTRAC must disclose "designated information" to the appropriate police force or to CSIS.[54]

---

49 *supra note 5*
50 *supra note 5*
51 *Ibid.*, sections 56.1(1)-(2).
52 *Ibid.*, section 58(2).
53 *Ibid.*, sections 55(1), 55(3).
54 Canada, *FINTRAC 2006 Annual Report*, (Ottawa: FINTRAC, 2006), online: FINTRAC <http://www.fintrac.gc.ca/publications/annualreport/2006/3_e.asp> [*Annual Report*].

FINTRAC thus holds discretion in terms of funnelling information to the RCMP and CSIS. It is not clear from the legislation whether FINTRAC would be justified in providing information to one of these entities alone. Furthermore, to what extent does FINTRAC coordinate efforts with these institutions? If these entities do share information, what is the nature of information sharing among them? For purposes of both efficiency and efficacy, this is a crucial practical consideration distinct from the precise legal provisions outlined above. In creating FINTRAC, a body that operates alongside but not necessarily in cooperation with CSIS and the RCMP, the *Proceeds of Crime Act* may contribute to an overall problem of inefficacy. FINTRAC's effectiveness will be affected by the degree of co-operation and information sharing between the RCMP and CSIS.

3. UNITED STATES

This section examines the main U.S. legislative provisions governing the financing of terrorism. These are the U.S. Criminal Code, the Patriot Act, the 1956 and 1957 money laundering statutes, and the Bank Secrecy Act. It will engage a comparison between Canadian and U.S. law and examine a key institutional structure present in the U.S. but not in Canada: the U.S. Office of Terrorism and Financial Intelligence.

U.S. Criminal Code

The U.S. Criminal Code contains a crime of terrorist financing which has been in place since 1994. The particular offense, contained in section 2339A, is entitled "Providing material support to terrorists", and reads as follows: "whoever …provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of [terrorist financing]…shall be fined… imprisoned not more than 15 years, or both, and if the death of any person results, shall be imprisoned for any term of years or for life…"[55]

The words "terrorist financing" are not contained in the section but the section includes by reference crimes listed in 18 USC 2332B dealing with violent crimes including "federal crimes of terrorism". Based on these provisions, the Department of Justice has stated that the term "terrorist financing" refers to the act of knowingly providing something of value

55 18 U.S.C. para2339A.

to persons and groups engaged in terrorist activity.[56] The term "material support or resources" is defined in section 2339A and includes "currency or monetary instruments or financial securities, financial services…" A similar offence, contained in section 2339B, exists for providing material to a foreign terrorist organization.[57]

There are two Executive Orders also relevant to terrorist financial networks. First is Executive Order 13224 entitled "Blocking Terrorist Property". This Order expands the U.S. Treasury's authority to freeze assets and U.S. transactions of persons or institutions associated with terrorists and terrorist organizations.[58] The Treasury can also freeze the assets of, and deny U.S. access to, foreign banks that refuse to cooperate. Second is Executive Order 13382, entitled "Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters". It provides the U.S. Treasury with authority aimed at freezing the assets of proliferators of weapons of mass destruction (WMD) and their supporters.[59]

As the Department of Justice has stated, the philosophical underpinning of the U.S. strategy since 9/11 has been "strategic overinclusiveness". It was felt that even humanitarian and charitable organizations will need to come within the law and a broad-based legal approach (further set out below) would be necessary to ensure this occurred. Finally, the U.S. did not want to have to trace moneys from the U.S. to their ultimate use.[60]

Patriot Act

The U.S. Patriot Act[61] provides federal officials with authority to track and intercept communications, and the Secretary of the Treasury with a legislative arsenal to combat corruption of U.S. financial institutions for foreign money laundering purposes. The Patriot Act contains a focus on banks as a conduit of money laundering by "hiding the identity of real parties in interest to financial transactions…".[62] The Act is also concerned with foreign government bodies as being potentially corrupt "particularly

---

56 18 U.S.C. para2339A. See also U.S. Department of Justice, "Terrorist Financing" (2003) Vol 51:4 http://www.usdoj.gov/usao/eousa/foia_reading_room/usab5104.pdf [*DOJ publication*].

57 18 U.S.C. para2339B.

58 Executive Order 13224 of September 23, 2001 "Blocking Terrorist Property" http://www.state.gov/s/ct/rls/fs/2002/16181.htm.

59 Executive Order 13382 of June 28, 2005 " Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters" http://www.fas.org/irp/offdocs/eo/eo-13382.htm.

60 *DOJ publication*, *supra* note at 8-9.

61 *USA Patriot Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 [*Patriot Act*].

62 *Patriot Act, ibid.*, section 302(6).

if those services include the creation of offshore accounts and facilities for large personal funds transfers to channel funds into accounts around the globe."[63]

Specifically under the Act, all financial institutions must create anti-money laundering programs. Treasury has the authority to impose information-gathering measures on business sectors that do not adhere to anti-money laundering standards imposed by regulators. The legislation appears more directly to regulate the private sector than does Canada's which simply imposes duties, the violation of which can result in criminal or regulatory prosecutions. Treasury has the authority to facilitate the sharing of suspicious activity reports with other countries, specifically, the intelligence communities in these countries. Measures exist to prevent individuals from purchasing financial anonymity, for example, through shell banks with no physical presence.[64]

The Patriot Act is balanced, because it ensures that any forfeitures made in connection with anti-terrorist efforts permits "for adequate challenge consistent with providing due process rights…"[65] The Canadian forfeiture provisions contemplate notice to those who are known to own or control property subject to forfeiture, some protections for innocent third parties who have exercised reasonable care to ensure that the property would not be used for terrorist purposes and appeals to the Federal Court of Appeal.[66]

The Patriot Act seeks to strengthen the ability of banks and other financial institutions to maintain the integrity of their employee population…"[67] Notably, there is recognition that cooperative efforts are necessary between private and public sector. The Act explicitly provides for cooperation among financial institutions, regulatory authorities, and law enforcement authorities on matters relating to financing of terrorist groups[68], including through the use of charities, nonprofits, and nongovernmental organizations.

---

63 *Ibid*., section 302(7).
64 Mariano-Florentino Cuellar, "The Tenuous Relationship Between The Fight Against Money Laundering and the Disruption of Criminal Finance" (2003) 93 J. Crim. L. & Criminology 311 at 362.
65 *Patriot Act*, *supra* note 62, section 302(8).
66 *supra note 62*
67 *supra note 3*
68 *Ibid*,. section 314(a)(2)(A).

It is not clear that the Canadian regime adequately addresses information sharing among governments as the U.S. clearly attempts to do with these legislative provisions.[69] However, information sharing, especially among governments and agencies at an international level, may undermine domestic prosecutions in Canada. This is especially the case if Canadian officials have received information from foreign agencies, and would be forced to disclose such information if they pursued the prosecution. Revealing such information may impede law enforcement activities in the foreign jurisdiction, and may strain relations with the foreign agency so as to undermine or sever the relationship that led to the information sharing in the first place.

Furthermore, although Canada has various layers of terrorist financing legislation in place, there is no apparent legal requirement that institutions and regulators operate in tandem or via joint efforts. While this cooperation may exist in practice, there would be undoubted benefits in discerning the extent of any existing cooperation (such as in the area of information sharing), and perhaps mandating such cooperation in law. As argued below, consideration should be given to whether there should be some sort of oversight of government's regulation of the private sector.

Money Laundering Statutes

Together with the registration and reporting requirements under the Patriot Act, the main pieces of legislation used to punish those who finance terrorism are two legislative provisions relating to money laundering.[70] Specifically, Section 1956 (referred to as the 1956 money laundering statute) criminalizes concealing criminal proceeds and promoting certain types of criminal conduct with monetary proceeds. Thus, if a person attempts or actually conducts a financial transaction that involves proceeds of a specified unlawful activity, and knows that the property involves proceeds of crime, this person will violate Section 1956(a)(1). Thus, the elements of the offence include: knowledge; existence of proceeds derived from unlawful activity; financial transaction; and, intent.[71] The Patriot Act expanded the category of specified unlawful

---

69 Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Ministry of Public Works, 2006) at 331[*Arar Events Report*]. While the Report does not engage in a U.S.-Canada comparative analysis on this issue, it does note that information sharing, done in a responsible manner, is vital, and recommended that the RCMP maintain and follow policies relating to information sharing. This issue is addressed *infra* section 4.

70 *Laundering of Monetary Instruments*, 18 U.S.C. section 1956 (1986).

71 See *e.g. United States v Sayakhom* 186 F.3d 928 at 942-43. See also Cuellar *supra* note 65 at 337-338.

activity that includes a list of "terrorism offences"[72] which includes financial transactions.[73] Section 1956(a)(2) also creates a separate crime targeting the international movement of money connected with some crimes.

Section 1957 targets conduct involving transactions with certain types of criminal proceeds. The section prohibits knowingly disbursing or receiving more than $10,000 of criminally derived proceeds if a financial institution is utilized. The elements of the offences are: (a) engaging or attempting to engage; (b) in a monetary transaction (which is defined to mean the use of a financial institution); (c) in criminally derived property; (d) valued at more than $10,000; (e) the property derives from specified unlawful activity (as defined under Section 1956); and, (f) the person knows that the property is criminally derived.[74]

We should note limits of this legislation and terrorist financing laws generally. In particular, acts of terrorism may be financed with funds that do not derive from criminal sources. The 9/11 Commission Report concluded that "it cost al Qaeda about $30 million per year to sustain its activities before 9/11 and…this money was raised almost entirely through donations."[75] The Report further concluded that al Qaeda had numerous sources of funding, and the authors of the report found no evidence that any person in the U.S., any foreign government, or foreign government official provided financial assistance to the hijackers.[76] The difficulty in finding evidence is not limited to the 9/11 attacks, but is likely pervasive in this area of law. It is not unreasonable to question, therefore, whether terrorist financing legislation is effective in preventing and combating terrorist activity.

The Bank Secrecy Act

The U.S. also has in play a system of regulatory rules and procedures aimed specifically at financial institutions. The main purpose of these rules is to create a reporting procedure to obtain information about suspicious transactions, and to provide for sanctions in the case of violating reporting procedures. Administered by the U.S. Treasury, the Bank Secrecy Act (formally the Currency and Foreign Transactions Reporting

---

72 *Supra note 62*
73 See 18 U.S.C. section 2332d (1996).
74 For discussion, see Cuellar *supra* note 65 at 342.
75 *Supra* note 65
76 *Supra note 37*.

Act)[77] contains a long list of institutions subject to the Act, including: state chartered commercial banks, post offices, casinos, and securities firms. It also provides discretion to the U.S. Treasury Department to define further the term "financial institutions".

Entities that fall within this definition must report any single currency transactions over $10,000, and multiple transactions over this amount that are conducted on the same day (if the institution knows that the transaction was conducted on behalf of the same person).

This reporting procedure resembles to some extent the process laid out in the current Proceeds of Crime Act but includes a broader list of obligated entities. Bill C-25 is more closely aligned with this U.S. statute, especially in its extension of the list of entities caught by the reporting obligation. However, Bill C-25 does not allow government agencies to define further the list of regulated entities and in this way is not as broad as the U.S. law.

Office of Terrorism and Financial Intelligence

Created in 2004, the U.S. Office of Terrorism and Financial Intelligence (OTFI) is a division of Treasury that consolidates the policy, enforcement, regulatory and international functions of the Treasury in the area of terrorist financing. The OTFI aims to detect the exploitation of financial systems by terrorists. It also allows implementation of regulatory enforcement programs (including sanctions) as well as cooperation with the private sector and international bodies against terrorist financing.[78]

The OTFI has as its main objective gathering and analyzing information from the intelligence, law enforcement, and financial communities regarding means by which terrorists earn, move, and store money. It has the ability to adopt policy, regulatory or enforcement actions to freeze assets of terrorists, prevent corrupt financial institutions from operating in the U.S. and trace and repatriate assets looted by corrupt foreign officials.[79] The OTFI advises the government in areas of combating rogue financial threats, including terrorism and weapons of mass destruction

---

77 P.L. 91-508, Titles I and II, as amended, codified at 12 USC 1829b – 1951059 (2000) and 31 USC 5311-5330 (2000). See also 31 C.F.R. section 103 (2002). See Cuellar, *supra* note 65 at 351-352 for discussion.

78 *Supra note 65*

79 United States Department of the Treasury, "Terrorism and Financial Intelligence Goals", United States Department of the Treasury <http://www.treasury.gov/offices/enforcement/goals.shtml>.

proliferation financing, money laundering and other financial crimes.[80] The Department of Treasury submits an annual Performance and Accountability Report to Congress. Contained in this report is a summary of the activities of the OTFI and other aspects of Treasury's efforts to combat the financing of terrorism (including a description of its activities relating to the administration of the Bank Secrecy Act).

Canada does not have a coordinating body of this nature and certainly does not have the many layers of infrastructure that the U.S. has in the area of anti-terrorist financing. While inefficiencies can emerge from centralization of this nature (per Posner discussed above), the question arises as to whether some type of body that coordinates would serve a useful function. In particular, it would be useful to contemplate the benefits of a body that oversees the efforts of the individual entities that play a role in curbing and monitoring terrorist financing. Such a body could, as in the United States, report to the legislature or legislative committees that could conduct a review of the effectiveness of regulation and the co-ordination of regulatory efforts.

4. ANALYSIS

A. Problems with Current Regime

Before we evaluate whether reforms to the current regime are necessary, we must understand problems underlying the regime. In this section, we turn to examine some of these issues relating to: efficacy of the current legal regime; information sharing; privacy rights; costs on private institutions; and, charities.

Efficacy. The Proceeds of Crime Act is, to a great degree, focused on private (as opposed to governmental) actors and compels them to undertake reporting and monitoring of suspicious transactions. The Act together with the amendments contained in Bill C-25 contain broad reporting obligations that apply to every financial transaction where there are reasonable grounds to suspect that the transaction is related to the "commission or attempted commission of a terrorist activity financing offence".[81] Thus, the obligation to report applies if such transaction

---

80 See United States Department of the Treasury, "Education Duties & Functions", online: United States Department of the Treasury < http://www.treas.gov/education/duties/treas/u-sec-enforcement.shtml>.

81 *Bill C-25, supra* note 2, section 5.

occurs or if the transaction is merely attempted. The provisions seem so broad that they conceivably capture any number of interchanges. A host of questions arise: Is it reasonable to expect that financial institutions will report all such interchanges? Is creating a statutory offence the best or only way to encourage the reporting? Should we devote resources to improving the capacity of financial institutions to spot suspicious transactions? How much of the financing of terrorist activities occur through the financial institutions subject to reporting requirements?

FINTRAC's Annual Report for 2005-06 states its results according to "case disclosures" each of which consists of a bundle of "designated information" about the individual or company involved in reportable transactions.[82] In its Report, FINTRAC states that 168 case disclosures were made: 134 of these were for suspected money laundering while 33 were for "suspected terrorist activity financing and/or other threats to the security of Canada". One case disclosure involved both of these items.[83] The Annual Report does not indicate to whom the case disclosures were made, only that the designated information must be disclosed to the appropriate police force or CSIS, as well as to the Canada Revenue Agency and the Canada Border Services Agency.[84]

The Annual Report also states that FINTRAC has improved the "sophistication and thoroughness of our analytical process" and has received a growing amount of information "from law enforcement and national security agencies."[85] The Report states that "Canadian financial institutions and other financial intermediaries are becoming more effective in detecting suspicious transactions".[86] The number of suspicious transaction reports is stated to have increased from 19,111 in 2004-05 to 29,367 in 2005-06.

Thus, in total there were 33 case disclosures on terrorism financing from almost 30,000 reports from financial institutions (.0011%). Despite the voluminous paperwork filed and received by FINTRAC, the result appears to be that only a minimal amount of disclosures relate to suspicious transactions. In addition, one must question what happens with these

---

82 *Supra note 2*
83 *Supra note 55*
84 *Ibid.* at 5.
85 *Ibid.* at 9.
86 *Ibid.* at 9.

33 disclosures. No pure financing prosecutions have been launched.[87] In short, given that the legislative system is based on information flows in and out of FINTRAC, it is imperative to know what happens with the information.

The mere fact that entities such as banks and other financial institutions report frequently does not indicate whether those entities that most need to report are in fact doing so or that the information that is being reported is in fact of significance. In order to determine whether the reporting mechanism is effective in weeding out suspicious transactions, we need to know whether the transactions were legitimately and actually "suspicious". The fact that they were reported does not make them so. The reality is that from these results it is unclear how effective FINTRAC has been in fulfilling its mandate to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities.[88] The case disclosures and information regarding suspicious transactions tell us nothing about whether an actual threat was curtailed. Were these cases resolved? Were these transactions legitimately labeled "suspicious"? While the information that FINTRAC receives may assist in detecting the targeted activities, there is nothing to indicate that FINTRAC has been successful in its deterrence role. [89]

The recent Senate Banking, Trade and Commerce Committee suggests that FINTRAC's numbers may be low. In a report issued in 2006, the Senate Committee concluded that the amount of dirty money laundered in Canada each year by criminals and terrorists "is probably in the tens of billions of dollars". [90] However, the Senate Committee completed no statistical examination of costs and benefits but focused instead on anecdotal reports from, and interviews with, various industry actors. The point remains, therefore, that until this time, there has been no concerted and comprehensive effort towards determining whether the current legislative regime is effective in preventing terrorism and the costs and benefits inherent in the regime.

---

87 Yet this does not necessarily mean that the 33 disclosures were ineffective in terms of disruption and surveillance. Reference is made to the case of *R. v. Khawaja* involving a section 83.03 charge of Mohammad Momin Khawaja who was arrested March 29, 2004 and accused of participating in the activities of a terrorist group, and facilitating a terrorist activity. See *R. v. Khawaja* [2006] O.J. No. 4245.

88 See *Annual Report*, *supra* note 55.

89 Supra note 55

90 Canada, Standing Senate Committee on Banking, Trade and Commerce, *Stemming the Flow of Illicit Money: A Priority for Canada,* (Ottawa: The Senate of Canada, 2006) at 1, online: Parliament of Canada < http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/bank-e/rep-e/rep09oct06-e.pdf> [*Senate Committee Report*].

Information Sharing. This issue has two aspects: first, inter-agency information sharing and, second, sharing between FINTRAC and entities that file reports with it. FINTRAC is the repository of a great amount of information relating to suspicious transactions. This includes reports of suspicious transactions from CSIS and the RCMP, as well as reports from customs officers and the Canada Revenue Agency (under Bill C-25). To what extent are these channels being utilized? Is there information sharing among agencies? If the RCMP is undertaking an investigation, to what extent will FINTRAC share information that may be relevant to the RCMP investigation? In what circumstances does FINTRAC pass information to CSIS and in what circumstances does it pass information to the RCMP? Do the RCMP and CSIS share the information that is passed on and do they co-ordinate their efforts with respect to terrorism financing? These issues require evaluation.

FINTRAC also receives information from financial institutions subject to the Proceeds of Crime Act. Under the current system, if one bank has reported suspicious activities, it likely does not know of possible similar suspicious activities by the same perpetrator at another bank that has also reported. It also may have no idea of whether any of the reports it filed with FINTRAC concerned entities that it needs to monitor going forward. This information sharing among institutions that are subject to the Proceeds of Crime Act would perhaps better enable them to carry out what is primarily a monitoring function (that seems to be overshadowed by a reporting obligation). At the very least it would make sense to have a system of "alerts" that FINTRAC provides to all financial entities once it receives suspicious reports upon which it (or other law enforcement channels) has acted.

The Senate Committee raised similar concerns in its recent report. The Committee contemplated that the legal regime may be more effective if there were a two-way flow of information between FINTRAC and law enforcement and intelligence agencies as well as between FINTRAC and the financial entities that report to it. The Senate Committee concluded, "more information shared among the parties would result in more effective detection and deterrence."[91] Representing certain financial entities, the Canadian Bankers' Association suggested to the Senate Committee that more feedback from FINTRAC would be useful in developing its reporting mechanisms.[92]

---

91 *Senate Committee Report, ibid.* at 16.
92 See *ibid*. citing comments from the Canadian Bankers' Association.

The main difficulty with information sharing, of course, is possible infringement of privacy rights as discussed below. Furthermore, even with a two-way flow of information, it is not clear whether such open channels prevent terrorist financing or assist in doing so. Even if some forms of terrorism financing are stopped, it is possible that terrorists will find other means to finance their activities.

Privacy Rights. Under the Proceeds of Crime Act, there is a prohibition on officials (of FINTRAC) to refrain from disclosing certain information contained in reports that are submitted or other information obtained under the Act.[93] However, this information may be disclosed where officers have reasonable grounds to suspect that the information "would be relevant to investigating or prosecuting…a terrorist activity financing offence."[94] This means that whenever an officer on reasonable basis suspects information to be relevant in an investigation, this information can be disclosed. Questions arise as to what constitutes "reasonable grounds". The Act and its proposed amendments do not provide guidance on what types of information are to be collected and what is the threshold for disclosure of collected information in the context of an investigation.

In terms of the entities that report under the Proceeds of Crime Act, the threshold for determining whether information should be reported is low and continues to decrease under Bill C-25. Listed entities must report every financial transaction that occurs or that is attempted. This means that the broad group of persons and entities caught by the reporting provision will be reporting transactions that provide reasonable grounds to suspect a terrorist financing activity, but which are not necessarily terrorist financing activities. In other words, a great many transactions may be reported that have no connection at all to terrorist financing. The concern is that otherwise private information is made public; and, more particularly, the private information of innocent customers is disclosed to FINTRAC, and possibly by FINTRAC if it passes on information to CSIS or the RCMP.

There has been criticism regarding the invasion of privacy brought about by the Proceeds of Crime Act, including the proposed amendments to the Act. The privacy concerns become even greater when we recognize that the Proceeds of Crime Act takes a broad-brush approach that results in many innocent transactions being reported. Some have suggested

---

93 *Proceeds of Crime Act*, *supra* note 5, section 36(1).
94 *Supra note 5*

creating an independent review commission with the powers and authority to conduct random reviews of FINTRAC's files and operations. Indeed, the Arar Commission recommended that the Security Intelligence Review Committee (SIRC) be given jurisdiction to review the national security activities of FINTRAC.[95] Administrative burdens and increasing expenses may weigh against the creation of such an agency. However, a strong case can be made that under the Act, intrusions into the affairs of individuals and businesses alike are extensive. The Senate Committee raised a similar point in its recent report, asserting that any legislative changes to the Proceeds of Crime Act must be considered with due regard to safeguarding the balance between the need for information that is reported on the one hand and the privacy of Canadians on the other.[96]

Costs. The private sector bears much, if not most, of the burden of in the legislative amendments designed to prevent financing of terrorists.[97] As discussed above, the main targets of reporting requirements under both Canadian and U.S. legislation are financial institutions. The Economist discusses compliance costs of this type of legislation in the UK context:

> The compliance costs for financial institutions are substantial. Graham Dillon of KPMG, a consultancy, reckons it costs each mid-tier bank in Britain £3m-4m ($5m-6m) to implement a global screening programme that involves regularly checking customer names--and those of third parties involved in their transactions--against United Nations embargo and American sanctions lists for possible terrorist matches. He reckons multinational banks each spend another £2m-3m per year to oversee implementation in their far-flung operations (such institutions commonly have 70 to 100 different transaction

95 *House of Commons Debates*, 067 (23 October 2006) at 4097 (Hon. Judy Sgro); Arar Inquiry Report, *supra* note 6 at 558.
96 *Supra note 6*
97 *Supra note 91*

> systems). In addition, "tens of millions of pounds" are spent each year in London alone on data storage and retrieval to satisfy a requirement that banks' client and transaction data be kept for five to seven years. Similar rules exist in America, Singapore and other European countries.[98]

This excerpt suggests that monitoring and reporting of terrorist financing activity is costly, and by implication, has the potential to threaten the economic activity of private businesses.[99] As suggested in the quote above, there will be increases in internal management costs and operational costs on banks themselves as they implement and enforce far-reaching reporting procedures such as those stipulated in the Proceeds of Crime Act. Organizations, especially smaller organizations, may disproportionately bear the reporting burden in terms of costs of monitoring and reporting.

On the other side of the transaction is the customer. If an individual knows that personal information regarding his or her financial transactions will be disclosed or reported, the individual may decide that he or she does not want to "do business" with the bank, despite the fact that the bank is not engaging in terrorist financing at all.[100] There is thus a potential loss of customer base under the legislative scheme. Though the regime is perhaps comprehensive in the reporting procedures it mandates, it may also detract from individuals' willingness to do business.

The Proceeds of Crime Act thus bears on firms' efficiency, where efficiency refers to cost-effectiveness. It raises the question of whether the costs of operating the business outweigh the benefits of doing so, and more broadly, whether the costs imposed under the legislation outweigh the benefits to be gained from the scheme. This second issue is an important question that must be raised in any assessment of the regime as a whole. Finally, the legislative regime may be responsible for sending financing of terrorist activities underground to *hawala* and other entities, i.e. away from banks and regulated entities.[101]

---

98 *Ibid*.
99 Kevin E. Davis, *supra* note 16 at 185.
100 *Supra note 16*
101 See Tom Naylor, *Satanic Purses* (Montreal: McGill-Queen's University Press, 2006) at 152-166.

Charities. Charities may have multifarious purposes, some of which are connected to financing terrorism. The charity as a whole, including the persons for whom the charity functions, can be negatively affected by the acts of some or one of its members. As Davis explains, "funds provided are likely to support both legitimate charitable activities and terrorist activity…subjecting either the organization or its supporters to the harsh sanctions contemplated by counter-terrorism legislation may be a disproportionate response to the threat they pose".[102] Furthermore, it is not clear that *mens rea* requirements under the Criminal Code could be met in a charity that inadvertently served as a conduit of funds but otherwise serves humanitarian purposes.

Nevertheless, FINTRAC's 2006 Annual Report states that one third of terrorism financing disclosures involved charities. Thus, perhaps the Bill C-25 amendments, which attempt to create channels of information between FINTRAC and the CRA, are warranted. However, information that can be obtained from the CRA will presumably be limited to registered charities as opposed to entities that purport to operate as non-profits or charities but that are not formally registered as such.

We should remember that organizations engaged in money laundering and/or financing terrorists may not be the type of organizations that view compliance with legal requirements (such as submitting the appropriate taxes and/or documentation with relevant authorities) as their foremost priority. The legislative regime (including the Bill C-25 amendments) may not be effective in combating terrorist financing; they may simply push more and more entities underground in order to achieve their objectives.

B. Directions

Assessing Efficacy. This report does not recommend implementing new laws under the Criminal Code or strengthening the Proceeds of Crime Act. Rather, its focus is on the need to assess the current regime to ensure that its infrastructure functions effectively. In particular, the recommendations relate to assessing the efficacy of the regime; establishing an oversight body for FINTRAC as well as creating an institution that coordinates all anti terrorist financing measures.

---

102 Davis *supra* note 16 at 184-185.

A full-blown evaluation of anti-terrorist financing laws has not occurred since their implementation a little more than five years ago. As stated in a submission to the Standing Senate Committee on Banking, Trade and Commerce examining Bill C-25, "the questions of proportionality (the extent to which the proposed measures are proportionate and commensurate with the risks at play) and necessity (the extent to which the measures are necessary based on empirical evidence) have not been appropriately addressed."[103] The time is ripe for such a review and, indeed, the federal government should not implement a new law unless and until the effectiveness of existing laws and institutions are assessed.

As noted above, there are crucial questions that should be examined regarding whether existing laws are effective not only in terms of increased information sharing but in providing to the RCMP and CSIS information that is useful in helping to prevent terrorism. FINTRAC states that it has received numerous reports under the Proceeds of Crime Act. However, it is not clear whether this body is actually catching those individuals who would be involved in terrorist financing. Furthermore, the Criminal Code contains relatively new provisions relating to terrorist financing and it is unclear whether these provisions are effective. Inherent in this assessment would be a statement of the objectives of terrorist financing legislation as a whole and the usefulness of the current means to achieve these objectives. Some questions to be examined are: do the various agencies that have charge over this area of law work co-operatively? If so, is such co-operation effective? If no, should there be an increased emphasis on co-operation?

It is recognized that assessing the impact and effectiveness of a regulatory instrument can be difficult. In the securities regulatory area, for instance, it has taken two decades of examining the low number of convictions in the insider trading area to reveal that either the regulatory regime is ineffective and/or the enforcement of the law has been weak.[104] On the contrary, terrorist financing law is relatively young, which makes evaluation of the efficacy of that law difficult. However, this does not mean that such an evaluation is not warranted, as discussed above. There are means to assess the legal regime. For example, to what extent do reports of suspicious transactions reveal information of actual terrorist financing? How many convictions have there been under the Criminal Code terrorist financing offences? Are the channels that are currently in

---

103 *Supra note 16*

104 William J. McNally & Brian F. Smith, "Do Insiders Play by the Rules?" (2003) 29 Can. Pub. Pol'y 125.

place for sharing of information among agencies being utilized? These crucial questions should be examined to assess the current regime. An assessment of the efficacy of existing terrorist financing law is necessary prior to implementing a new law designed to combat the financing of terrorists and terrorist activities.

Methodology. Apart from responding to these important questions, it may be useful to conduct either a cost-benefit analysis (CBA) or regulatory impact assessment (RIA) with regards to the current regime. In the securities regulatory field, the U.S. Securities and Exchange Commission, and to a lesser extent the Ontario Securities Commission, routinely incorporate CBA into their rule-making procedure. These CBAs are not usually based in statistical analyses and are qualitative in form.[105] In light of the difficulties in determining whether the regime has been effective in combating the financing of terrorist activity, it is useful to ascertain the benefits of the regime and whether these benefits outweigh its costs. The methodologies for undertaking the CBAs can be complex but they should be explored in the context of assessing the efficacy of the current anti-terrorist financing regime.

Admittedly, while it is possible to be specific in explaining costs and benefits, it is not the case that all costs and benefits are comprehensible or, for that matter, quantifiable. A further weakness of CBA is the variable criteria on which it is based. In light of this problem as well as the difficulty in quantification of costs and benefits, it is worthwhile considering other means of assessing the impact of regulatory initiatives. RIA is a technique that includes CBA but also involves a broader risk-based analysis than CBA entails. CBA does not typically weight risks. That is, it does not consider risk from the standpoint of the relative likelihood of facing specific costs or attaining certain benefits for various relevant stakeholders. For this reason, it may be biased in favour of more regulation since estimated costs of regulation are usually more certain than perceived benefits.

The following steps are often included in an RIA: identifying and quantifying the impact of the legislation; isolating alternatives, which may be non-law based, to address the problem; undertaking risk-based analysis; and, consulting affected parties. RIA also addresses benefits that may not be quantifiable – such as equity and fairness – which are

---

105 The SEC's use of CBA has been referred to as inadequate and some argue that it has lowered the quality of SEC rulemaking. See Edward Sherwin, "The Cost Benefit Analysis of Financial Regulation" (2005) http://www.law.harvard.edu/faculty/hjackson/projects.php.

important, especially from an public interest and protection standpoint. RIA examines the impact that a law has had as well as various alternatives. Who is impacted by the law and what is the range of impact across sectors? RIA is used in the UK which may be a useful jurisdiction to look to in obtaining precedents for such an analysis.

To complete an analysis of costs, benefits and risks (whether in the context of CBA or RIA) it will be necessary for the reviewer to have access to otherwise confidential information. For example, information is generally unavailable regarding the 33 case disclosures made by FINTRAC on terrorism financing. We are unsure whether FINTRAC funneled information relating to these 33 cases to the RCMP or CSIS or both and ultimately what happened with regards to these cases. However, this would be very important information in assessing the efficacy (benefits) of the regime.

In deciding how best to complete an assessment of Canada's terrorist financing regime, the usefulness of Cost Benefit Analysis and Regulatory Impact Assessment should be taken into account.

Oversight Body. Canadian law relating to combating terrorist financing is contained in the Criminal Code and in the Proceeds of Crime Act. The Director under the Proceeds of Crime Act is required to report to the Minister "from time to time" on the exercise of the Director's powers and to keep the Minister informed of "any matter that could materially affect public policy of the strategic direction of the Centre."[106] However, no body undertakes an assessment of the efficacy of the existing regime. Indeed, in the absence of such an assessment mechanism, there appears to be an assumption that the regime is effective. Furthermore, Canada has no institution that coordinates the efforts aimed at combating terrorist financing provided under these two pieces of legislation. Terrorist financing also impacts on multiple ministries and agencies within government, making co-ordination and information sharing more difficult. This is unlike the U.S. model where the Office of Terrorism and Financial Intelligence is a body that consolidates the policy, enforcement, regulatory and international functions of the U.S. Treasury relating to terrorist financing.

---

106 *Proceeds of Crime Act*, *supra* note 5, sections 52(1)-(2).

With regards to Canadian federal initiatives to combat terrorist financing, there is certainly the potential for coordination (particularly in the area of information sharing) among Canadian institutions such as FINTRAC, the RCMP, CSIS etc. For efficiency purposes, it stands to reason that information sharing and other forms of cooperation should occur, and, perhaps should be mandated. Legal parameters that govern information sharing among these agencies may need to be established to ensure that the information sharing occurs "in a reliable and responsible fashion".[107] An oversight or umbrella organization that coordinates the activities of these various institutions may also be warranted.

Some may look to FINTRAC as capable of coordinating activities among the various institutions at work in combating terrorist financing. However, FINTRAC's mandate is limited to the Proceeds of Crime Act and terrorist financing law clearly extends beyond this one statute. Furthermore, in light of the privacy and efficacy issues raised in this report, it stands to reason that there should be a separate body that oversees FINTRAC's operations. This independent reviewer would be responsible not only for evaluating the activities of FINTRAC but also for coordinating all of the laws relating to the financing of terrorism and perhaps assessing the effectiveness of the current regime. As the Auditor General has stated, "the government should assess the level of review and reporting requirements to Parliament for security and intelligence agencies to ensure that agencies exercising intrusive powers are subject to levels of external review and disclosure proportionate to the level of intrusion."[108]

The question remains as to who the independent reviewer should be. There are a number of options here beginning with the Auditor General, some sort of Ministerial oversight, Parliamentary Committee, or SIRC. Notably, the Arar Inquiry Report recommended that SIRC's role should be expanded to review national security activities of FINTRAC.[109] However, SIRC deals mainly with issues of propriety, its mandate being to "review generally the performance of the Service [CSIS] of its duties and functions".[110] In light of the argument here in favour of an oversight body that can deal with issues of efficacy, it appears that SIRC may not be the appropriate body to perform this oversight role. Further study is warranted on whether existing institutions are able to take on this oversight function and how the oversight will be performed.

---

107 *Supra note 5*
108 *Supra note 7*
109 *Arar Events Report, supra* note 7 at 573.
110 *Supra note 7*

Study should be accorded as to whether an oversight body is warranted to consolidate the policy, enforcement and regulatory processes currently in place to combat terrorist financing, and, if so, whether existing institutions are able to take on this oversight function and how the oversight will be performed.

Overseeing FINTRAC. FINTRAC receives information from various sources (CBSA, CSIS, RCMP) but is permitted to disclose only certain designated information. The structure of FINTRAC, and these rules in particular, are meant to balance competing objectives. The result however is a body that lacks transparency, as the recent Arar Inquiry Report pointed out.[111] For a number of reasons, it makes sense to have a body that oversees FINTRAC and that examines a variety of questions on a periodic basis. First, is FINTRAC performing its functions effectively (per the above discussion)? Second, to what extent are privacy rights sacrificed? Third, is FINTRAC complying with the statute that provides its mandate and is it administering the statute appropriately? Finally, should more information sharing occur?

At present, FINTRAC is subject to certain oversight procedures in the Proceeds of Crime Act. Specifically, it must submit an annual report on its operations to the Minister and the Minister will table a copy of the report in Parliament.[112] In addition, the administration and operation of the Act will be subject to a five-year review by a committee of Parliament under Bill C-25.[113] All receipts and expenditures of FINTRAC are subject to examination and audit.[114] Although FINTRAC can be the subject of suits and legal proceedings,[115] no action lies against any of the employees of the Centre if they have acted in good faith in discharging their duties.[116]

While the Act will be reviewed every five years by a Committee of Parliament, there is no body that reviews FINTRAC's operations and the efficacy of those operations. There is some merit, therefore, in having a review committee with the powers and authority to conduct random reviews of FINTRAC's files, operations and compliance with its governing statutes and other law. This is a recommendation made by the Senate

111 *Arar Events Report*, *supra* note 7 at 567.
112 *Supra note 7*
113 *Supra note 5*
114 *Proceeds of Crime Act, supra* note 5, section 70(1).
115 *Supra note 5*
116 *Ibid.,* section 69.

Committee on Banking Trade and Finance which stated that FINTRAC should be subject to an annual review, and the reviewing body should be SIRC.[117] While this report makes no suggestion regarding the precise body that takes on the oversight function, it does point to the necessity of such an overseer.

Consideration should be given to the issue of whether an oversight body that monitors the activities of FINTRAC with respect to its efficacy as well as the propriety of its operations on a periodic basis is warranted.

Admittedly, a danger exists in focusing only on FINTRAC in the proposed review and monitoring system. Presumably, such a review would focus only on the flow of information into and out of FINTRAC but not necessarily on actions taken with respect to that information once it is handed over to other bodies such as the RCMP, CSIS or foreign agencies. Thus, in keeping with the discussion throughout this section, the oversight body should be charged not only with monitoring FINTRAC, but also with overseeing all entities that play a role in anti-terrorist financing activities including those of CSIS and the RCMP.

5. CONCLUSION

The Canadian regime that governs the financing of terrorism is relatively new – it has been in existence for less than a decade. It is difficult to know at this time whether the regime has been and is effective in combating the financing of terrorism. However, this is not to say that the regime is ineffective. Rather, before any new law is implemented, an assessment of the efficacy and efficiency of the current regime is required. This assessment would be a first step towards understanding whether (and where) additional laws are necessary. This is a pragmatic approach. Our expectations about what law can achieve should be reasonable and well informed. That is, we should not advocate a specific set of legal reforms in the absence of evidence that this particular reform (as opposed to other available alternatives) is warranted. This is because regulation is costly in the sense that it imposes burdens on the regulated. Those burdens may indeed be justified but they must be proven to be so. Otherwise, the regulation is nothing more than an experiment, and usually a costly one.

---

117 *Senate Committee Report*, *supra* note 91 at 22.

Anita Indira Anand, BA (Hons) (Queen's) 1989, BA (Hons in Jurisprudence) (Oxon) 1991, LLB (Dalhousie) 1992, LLM (Toronto) 1996, joined the University of Toronto Faculty of Law from Queen's University where she was an Associate Professor (2003-2006) and Assistant Professor (1999-2003). She currently serves as Associate Dean (JD Program) at the Faculty of Law at Toronto. In 2006, she was a Canada-U.S. Fulbright Scholar and Visiting Olin Scholar in Law and Economics at Yale Law School. During the Fall 2005, she was a Visiting Lecturer in Law at Yale Law School where she taught comparative corporate governance. She is the recipient of research grants from the Social Sciences and Humanities Research Council of Canada (two awards) and the Foundation for Legal Research (three awards) as well as the Canadian Association of Law Teachers' Scholarly Paper Award (2003). In Fall 2004, she received the Queen's Law Students' Society Award for Excellence in Teaching and in Fall 2006, she and co-authors Frank Milne and Lynnette Purda were awarded the Best Paper in Managerial Finance by the International Journal of Managerial Finance for their empirical research relating to corporate governance. She has published articles in the University of Toronto Law Journal, the McGill Law Journal, the Delaware Journal of Corporate Law, the Stanford Journal of Law, Business and Finance, the NYU Journal of Law and Business and has co-authored the book *Securities Regulation: Cases, Notes and Materials* with Mary Condon and Janis Sarra. Professor Anand has conducted research for the Five Year Review Committee, the Wise Person's Committee, and the Task Force to Modernize Securities Legislation in Canada. She is the Editor of Canadian Law Abstracts, published by the Legal Scholarship Network and the Vice President (President Elect) of the Canadian Law and Economics Association. Her main research and teaching areas are corporate law, securities regulation, and bankruptcy and insolvency law.