Briefing Book

PREPARED FOR THE SPECIAL SENATE COMMITTEE ON ANTI-TERRORISM

RECENT DEVELOPMENTS IN ANTI-TERRORISM LAW AND POLICY IN THE UNITED KINGDOM, UNITED STATES, AUSTRALIA AND FRANCE

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

5 August 2010

FORWARD

The four papers contained in this briefing book provide a brief overview of recent developments in anti-terrorism law and policy in the United Kingdom (UK), United States (US), Australia and France. They provide an outline of the legislative framework each of these countries has put in place to combat and prevent terrorism, and highlight some of the recent case law developments with respect to the terrorism provisions each country has enacted. The papers also provide an update on some of the recent policy initiatives that these four nations have put into place to deter homegrown terrorism.

CONTENTS

CANADA

PREPARED FOR THE SPECIAL SENATE COMMITTEE ON ANTI-TERRORISM

RECENT DEVELOPMENTS IN ANTI-TERRORISM LAW AND POLICY IN THE UNITED KINGDOM

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

5 August 2010

INTRODUCTION

This paper provides an overview of some of the recent developments in anti-terrorism law and policy in the United Kingdom (UK). It outlines the legislative framework that the UK has put into place to combat and prevent terrorism, and highlights some of the recent case law developments regarding terrorism provisions contained in various statutes. The paper also provides an update on some of the recent policy initiatives that the UK has put into place to deter home-grown terrorism.

LEGISLATIVE FRAMEWORK AND RELEVANT CASE LAW

There are currently six main pieces of legislation in force in the UK dealing with terrorism.[1] The key provisions of these statutes are described below, along with some of the important case law developments respecting these provisions.

A. *Terrorism Act 2000*[2]

The *Terrorism Act 2000*, which was enacted prior to the bombing of the World Trade Centre in New York, New York, on 11 September 2001, superseded and replaced two other statutes that the UK Parliament had previously enacted to deal with terrorism: the *Prevention of Terrorism (Temporary Powers) Act 1989*[3] and the *Northern Ireland (Emergency Provisions) Act 1996*.[4] Both of these statutes required periodic renewal or re-enactment in order to remain in force. By contrast, except for one part related to Northern Ireland, the provisions contained in the *Terrorism Act 2000* are permanent.

One of the key provisions of the *Terrorism Act 2000* is the definition of "terrorism" itself, which is incorporated by reference into the other anti-terrorism statutes enacted by the UK government.[5] The Act also empowers the Home Secretary to create a list of "proscribed organizations" connected to terrorism (sections 3 to 10) and creates the offences of belonging to a proscribed organization, supporting a proscribed organization and wearing an item of clothing such as to arouse reasonable suspicion that one is a member or supporter of a proscribed organization (sections 11 to 13). In addition, the *Terrorism Act 2000* introduced provisions allowing for detention without charge (initially for a period of

---

1 Statistics on the use of various UK terrorism provisions found in several of the relevant statutes, as well as statistics on the outcomes of terrorism cases, are available on the Home Office's website at http://rds.homeoffice.gov.uk/rds/hosbpubs1.html.

2 (UK), 2000, c. 11. This statute is available at http://www.opsi.gov.uk/acts/acts2000/ukpga_20000011_en_1.

3 (UK), 1989, c. 4.

4 (UK), 1996, c. 22.

5 For information as to how "terrorism" is defined in this Act, and how this definition of terrorism compares to the definition of "terrorist activity" found in Canada's *Criminal Code*, please see Jennifer Bird, *Definitions of Terrorism in Canada, the United Kingdom, the United States, Australia and France*, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 4 October 2006 (a paper prepared for the Special Senate Committee on Anti-terrorism).

up to 7 days[6]) of those suspected to be terrorists (section 41), and allowed the police and the Home Secretary to define an area in the country and time period wherein police officers could stop and search any vehicle or person and seize articles of a kind which could be used in connection with terrorism (sections 44–47). The police were not required to have reasonable suspicion that an offence has been committed before exercising stop and search powers under sections 44 to 47.

It is important to note, however, that on 12 January 2010, in the case *Gillan and Quinton* v. *The United Kingdom,*[7] the European Court of Human Rights (ECHR) ruled that the stop and search powers contained sections 44 to 47 violated Article 8 of the *European Convention on Human Rights* (the Convention),[8] which guarantees the right to respect for privacy and family life, and that interference with this right, which can be permitted when such interference is determined to have been conducted "in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country," was not "in accordance with the law" because the provisions lacked appropriate safeguards to protect people against arbitrary interference with their right to privacy. The Court ordered the UK government to pay costs in the amount of 33,850 Euros to the claimants.

The ECHR's decision in *Gillan and Quinton* v. *The United Kingdom* runs counter to a 2006 House of Lords decision in the same case, in which the House of Lords upheld the legality of the stop and search powers contained in the *Terrorism Act 2000*.[9] However, in his most recent report, Lord Carlile of Berriew, who was appointed the Independent Reviewer of the *Terrorism Act 2000* more than eight years ago, and who publishes yearly reports on this piece, as well as other pieces, of terrorism legislation, was highly critical of the continued use by the UK of the stop and search powers found in section 44 of this Act, in particular, stating:

> Although the UK government is seeking permission to appeal *Gillan* to the Grand Chamber [of the European Court of Human Rights], preparations should be made for the potential failure of that appeal. I would go further. In my view the judgment already given has illustrated the excessive nature and use of *section 44*. Given the clearly expressed policies of the coalition partners prior to the 2010 General Election, I suggest that the time has arrived for the section to be repealed, and replaced by a more limited provision to deal with three broad sets of circumstances, These are:
>
> (a) counter-terrorism operations such as searches, arrests and some surveillance situations;

---

6 The pre-charge detention period was extended, by amendment to 14 days in 2003, and then to 28 days in 2006. The Labour Government of Prime Minister Tony Blair had attempted to amend the period of pre-charge detention to up to 90 days, but this amendment was defeated in the House of Commons and a 28 day detention period was substituted for the original 90 day proposal.

7 [2009] ECHR 28.

8 CETS No. 5, Rome, 4 November 1950.

9 It is important to note that the ECHR has no power to overrule the decisions of national courts, or overturn national laws, although its judgments tend to be influential at the national level.

> (b) some iconic events where there is security services advice of heightened threat or risk;
>
> (c) a closed (i.e., secret), regularly reviewed and unexaggerated list of true critical national infrastructure sites.[10]

On 8 July 2010, the UK government responded to the ECHR's decision in *Gillan and* Quinton v. *The United Kingdom*, as well as the criticisms of Lord Carlile of Berriew and others, by implementing new interim guidelines for the use of stop and search provisions under section 44. The new guidelines provide that the police may only stop and search vehicles and persons under this section of the Act if they reasonably suspect the person of terror-related activities. These new guidelines will remain in place until such time as the UK government conducts a further review of its terrorism legislation.[11]

B. *Anti-terrorism, Crime and Security Act 2001*[12]

The *Anti-terrorism, Crime and Security Act 2001* was enacted following the events of 11 September 2001. Some of its key provisions include: enabling law enforcement agencies to freeze assets of suspected terrorists at the beginning of an investigation to prevent the funds from being moved or used (Part 1, Schedules 1 and 2 of the Act); empowering the Treasury Department to make freezing orders in certain circumstances (Part 2 of the Act); granting police and security services, including foreign agencies, the power to ask public bodies, such as schools, hospitals, customs and inland revenue to disclose personal records during terrorism and criminal investigations (Part 3 of the Act); and enabling the Home Secretary to indefinitely detain, without charge or trial, foreign nationals suspected of terrorism (Part 4 of the Act).

It is important to note, however, that Part 4 of the *Anti-terrorism, Crime and Security Act 2001* was repealed and replaced by the control order regime introduced by the *Prevention of Terrorism Act 2005*,[13] following the House of Lords decision in *A (FC) and others* v. *Secretary of State for the Home Department*.[14] In that decision, the majority of the Court ruled that detaining foreign nationals indefinitely, on suspicion alone, violated Article 5 of the *European Convention on Human Rights,* which guarantees the right to liberty and security of the person, since the detention regime did not require the person to be brought to trial within a reasonable time, or alternately, to be released. The majority also found that the detention regime violated Article 14 of the Convention, which guarantees freedom of discrimination on several grounds, one of which is nationality, since the detention

---

10 Lord Carlile of Berriew, Q.C., *Report on the Operation in 2009 of the Terrorism Act 2000 and of Part 1 of the Terrorism Act 2006*, July 2010, presented to the UK Parliament pursuant to section 36 of the *Terrorism Act 2006*, at para. 54. This report is available at http://www.homeoffice.gov.uk/publications/counter-terrorism/independent-reviews/ind-rev-terrorism-annual-rep-09?view=Binary.

11 See Drew Singer, "UK strengthens test for stop and search of terror suspects," 8 July 2010, available http://jurist.org/paperchase/2010/07/europe-rights-court-orders-stricter-test-for-stop-and-search.php.

12 (UK), 2001, c. 24.

13 (UK), 2005, c. 2.

14 [2004] UKHL 56.

regime established by the *Anti-terrorism, Crime and Security Act 2001* treated foreign nationals differently than UK citizens.[15]

C. *Prevention of Terrorism Act 2005*[16]

As stated above, the *Prevention of Terrorism Act 2005* created control orders in response to the House of Lords decision in *A (FC) and others* v. *Secretary of State for the Home Department.* Control orders are civil orders made by the Home Secretary, or the High Court or Court of Session, against individuals, regardless of whether they are UK citizens or foreign nationals, in circumstances where there are reasonable grounds to suspect that individuals are involved in terrorism related activity.

There are two types of control orders: derogating and non-derogating control orders. The former must be made by a court, and allow for derogation from Article 5 of the *European Convention on Human Rights*. A more exacting standard of proof is required before a derogating control order may be made by the court than when a non-derogating control order is made by the Home Secretary. In addition, derogating control orders may only be made for 6 months at a time, whereas non-derogating control orders may be made for 12 months at a time. Special advocates may be appointed to represent individuals in control order proceedings and are given access to evidence that has not been made available to the person against whom the control order has been made, for reasons of national security. Information used to justify the imposition of a control order on an individual may also include information obtained by torture, provided that the torture occurred outside of the UK. Once a control order has been made, a range of restrictions may be imposed on the individual concerned, including house arrest, electronic monitoring, restrictions that prevent individuals from attending certain location or using cell phones or computers, and so forth.[17]

The control order regime in the UK has been subject to repeated court challenge, and in an October 2009 decision, *Secretary of State for the Home Department* v. *AF and another (No. 3)*,[18] the House of Lords concluded that the imposition of control orders to detain terrorism suspects will violate Article 6(1) the *European Convention on Human Rights*, which guarantees the right to a fair and public hearing within a reasonable time by an independent and impartial tribunal, if the Home Secretary, in the interests of national security, does not disclose sufficient information to the person concerned to allow him or her to know the case against them. In this case, the House of Lords, while not ruling the control order system itself to be invalid, remitted the cases of two of the three individuals

---

15 For a more detailed explanation of the decision of the House of Lords in *A (FC) and others* v. *Secretary of State for the Home Department*, please see Jennifer Bird, *Special Advocates in the United Kingdom (UK)*, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 18 November 2008, p. 7 (a paper prepared for the Special Senate Committee on Anti-terrorism).

16 Supra note 13.

17 For a more complete description of the control order regime and the role that special advocates play within this regime, see Jennifer Bird, *Special Advocates in the United Kingdom (UK),* Parliamentary Information and Research Service, Library of Parliament, Ottawa, 4 October 2006 (a paper prepared for the Special Senate Committee on Anti-terrorism), supra note 15.

18 [2009] UKHL 28.

appearing before them back to the High Court for a re-hearing, wherein the Home Secretary would be required to make further disclosure to these two individuals or rescind the control orders made against them.

In coming to its decision, the House of Lords was influenced by the February 2009 decision of the ECHR in *A and Others* v. *United Kingdom*,[19] in which that Court held that, even in cases where there are national security interests at stake, it may not be acceptable to withhold evidence that provides the grounds for suspicion in a terrorism case, at least in circumstances where doing so prevents persons from being able to effectively challenge the allegations against them.

More recently, in June of 2010, the UK Supreme Court ruled that another control order issued against another terrorism suspect was invalid because it found that the restrictions imposed on the individual made subject to it (a 16 hour curfew, and requiring the individual in question to live 150 kilometres away from his family) were too onerous, breaching his right to liberty under Article 5 of the *European Convention of Human Rights*,[20] and in July of 2010, the UK Court of Appeal ruled that two terrorism suspects could sue the government for damages over control orders which courts had determined had been wrongfully imposed upon them.[21] The UK government has since announced its intention to appeal this last judgement to the UK Supreme Court.[22]

Despite these recent court decisions which call into question the utility and legality of control orders, in his most recent review of the *Prevention of Terrorism Act 2005*, Lord Carlile of Berriew, who also conducts yearly independent reviews of this Act, concluded that "the control orders system remains necessary, but only for a small number of cases where robust information is available to the effect that the suspected individual presents a considerable risk to national security and conventional prosecution is not realistic."[23]

The control order system outlined in the *Prevention of Terrorism Act 2005* expires at twelve month intervals unless re-enacted (section 13). A vote on whether or not to re-enact the relevant provisions is currently scheduled for the spring of 2011.

---

19 Application No 3455/05 (unreported), 19 February 2009.

20 *AP* v. *Secretary of State for the Home Department*, [2010] UKSC 24. It is important to note that on 1 October 2009, the House of Lords, the highest appeal court in the United Kingdom, changed its name to the Supreme Court of the United Kingdom, pursuant to Part 3 of the *Constitutional Reform Act 2005*, (UK), 2005, c. 11. It did not change the membership of the court, but merely moved the Law Lords (12 professional judges appointed to the House of Lords to carry out that Chamber's judicial functions), out of the House of Lords and into a separately constituted court.

21 *AN* v. *Secretary of State for the Home Department,* [2010] EWCA Civ 869.

22 See Daniel Richey, "UK appeals court rules terror suspects may sue over wrongful control," 28 July 2010, available at http://jurist.org/paperchase/2010/07/uk-appeals-court-rules-terror-suspects-may-sue-over-wrongful-control-orders.php.

23 Lord Carlile of Berriew, Q.C., *Fifth Report of the Independent Reviewer Pursuant to Section 14(3) of the Prevention of Terrorism Act 2005*, February 2010, at para. 1. This report is available at http://www.official-documents.gov.uk/document/other/9781849871518/9781849871518.pdf.

D. *Terrorism Act 2006*[24]

The *Terrorism Act 2006* statute serves to criminalize certain actions that one might consider preparatory to the commission of an actual terrorist act. For example, the Act makes it a criminal offence to encourage terrorism by directly or indirectly inciting others to commit terrorist acts. Prohibited types of encouragement include the "glorification of terrorism" or the celebration of terror in such a way as may encourage others to commit terrorist acts (section 1). The Act also grants the Home Secretary powers to ban or proscribe groups that glorify terror and to prevent proscribed organizations from using front organizations to continue operating (sections 21 and 22). In addition, the Act creates new offences prohibiting the selling, loaning, distribution or transmission of terrorist publications (section 2), and prohibits the giving and receiving of training in terrorist techniques (section 6), attending terrorist training camps (section 8) and preparing to commit or preparing to assist in the commission of terrorist acts (section 5).

Of all of the terrorism statutes enacted by the UK Parliament in the last 10 years, the *Terrorism Act 2006*, with its emphasis on preparatory acts, seems most particularly targeted to combat home-grown terrorism. According to Lord Carlile of Berriew's most recent report as the reviewer of the *Terrorism Act 2006*, six suspects have been charged with an encouragement of terrorism offence: three in 2007–2008 and three in 2008–2009, with the charges resulting in two convictions.[25] He states in his report:

> I remain un-attracted by the use (uniquely in this legislation) of the word *'glorifies'*, it is linked so closely to the more conventional inchoate concept of incitement that the criminalisation of the conduct described is proportionate. I think I reflect judicial opinion that it is desirable that as many prosecutions as possible should be linked to specific terrorism acts and conspiracies. Juries are less likely to convict of less specific offences like these.
>
> Prosecution is an instrument of last resort against radicalisation. The *'Prevent'* strand of counter-terrorism strategy recognises this. It is better by far to discuss and persuade at community level, so that those minded to radicalise or to be radicalised have the opportunity to consider and reflect upon their own and their community or group's interests before charging offences under section 1.[26]

A brief description of the UK's Prevent Counterterrorism Strategy will be provided in a later section of this paper.

---

24 (UK), 2006, c. 11.

25 Lord Carlile of Berriew, Q.C., *Report on the Operation in 2009 of the Terrorism Act 2000 and of Part 1 of the Terrorism Act 2006*, July 2010, supra note 10 at para. 276.

26 Ibid. at paras. 276 and 277.

E. *Counter-Terrorism Act 2008*[27]

The *Counter-Terrorism Act 2008* appears to have been primarily designed to give police and other officials enhanced information gathering and information sharing powers for counter-terrorism purposes and to make further provision for the detention and questioning of terrorist suspects.

Key provisions found in the Act allow for the post-charge questioning, by a judge, of persons charged with terrorism offences or where the judge considers the offence to have a terrorist connection. The same set of provisions enable courts to draw an adverse inference from a suspect's refusal to reveal something during post-charge questioning later relied on in court (Part 2). Committing an offence with a "terrorist connection"[28] is also considered to be an aggravating factor at the time of sentencing. Other key provisions allow the police to request monitoring information from convicted terrorists and prevent them from foreign travel (Part 4), to collect DNA and fingerprints from individuals subject to control orders (sections 10 to 18), and adds to the definition of terrorism, an act committed for the purpose of advancing a "racial" cause, in an addition to a political, ideological or religious cause (section 73).

F. *Terrorist Asset Freezing (Temporary Provisions) Act 2010*[29]

The *Terrorist Asset Freezing (Temporary Provisions) Act 2010* was enacted in response to *Her Majesty's Treasury (Respondents)* v. *Mohammed al-Ghabra (FC) (Appellant)*,[30] a January 2010 decision of the UK Supreme Court. In that decision, the Court found certain Orders in Council made pursuant to *United Nations Act 1946*,[31] which served to freeze the assets of certain individuals listed on a United Nations list of terrorist entities created pursuant to United Nations Security Council Resolution 1267,[32] were outside the jurisdiction of the executive branch of government to make, because the *United Nations Act 1946* was not intended to authorize coercive measures which interfere with fundamental rights without Parliamentary scrutiny and because the Orders in Council allowed assets to be frozen on the basis of mere suspicion. The Court quashed the orders in question, pointing out that the government could have used the asset freezing provisions contained in the *Anti-terrorism, Crime and Security Act 2001*, which contained a more exacting standard of proof, to achieve the same result. The *Terrorist Asset Freezing (Temporary Provisions Act) 2010* was therefore enacted to ensure that the asset freezing Orders in Council made under the *United Nations Act 1946* continue to remain valid until December 2010, at which point the UK Parliament will have to consider how to alter these provisions in order to ensure that the UK meets its international obligations under United Nations Security Council Resolution 1267.

---

27 (UK), 2008, c. 28.

28 An offence is considered to have a "terrorist" connection if it is committed in the course of an act of terrorism or is committed for the purposes of terrorism. See section 93 of the *Counter-Terrorism Act 2008*.

29 (UK). 2010, c. 4.

30 [2010] UKSC 1.

31 (UK), 9 & 10 Geo. 6, c. 45.

32 United Nations Security Council Resolution 1267 calls on states to prohibit dealings with Osama bin Laden, Al Qaida and the Taliban.

POLICY INITIATIVES

Following the 7 July 2005 suicide bombings which took place on London's public transit system (three bombs exploded in the London Underground, while one exploded on a double-decker bus), and revelations, following these bombings that the acts were carried out by UK nationals, the UK government began to focus more of its attention on the challenges presented by home-grown terrorism. In the wake of these bombings, the government drafted and introduced the *Terrorism Act 2006*, which came into force in April 2006. As indicated above, of the six pieces of anti-terrorism legislation currently in force in the UK, the *Terrorism Act 2006* criminalizes certain types of activity that one might consider preparatory to the commission of actual terrorist acts, such as prohibiting the glorification of terrorism, the dissemination of terrorist propaganda, and attending terrorist training camps.

However, the UK government has also put other policies in place which would assist them in combating home-grown terrorism, whether directly or indirectly. Two of the key steps that the UK government has taken in this regard have been:

1. **Deciding to make its national security strategy publicly available.** The UK published its first national security strategy in 2008,[33] following up with an updated version of this strategy in 2009.[34] The 2010 strategy is expected to be published by the UK's new coalition government in the near future. While these 2008 and 2009 strategies are comprehensive, dealing with many issues other than the threat of home-grown terrorism, or even the threat of terrorism generally, both contain a summary of the steps the UK has been taking to combat home-grown terrorism.[35]

2. **Development of the CONTEST counter-terrorism strategy.** The UK Home Office developed its first comprehensive counterterrorism strategy, known as CONTEST in 2003, and updated this strategy significantly in 2009 (the 2009 strategy is often referred to as CONTEST TWO).[36] According to the UK government's 2010 Annual Report to Parliament with respect to this strategy, the CONTEST counter-terrorism strategy aims "to reduce the risk to the UK and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence."[37]

---

33 See Cabinet Office, *The National Security Strategy of the United Kingdom: Security in an interdependent world* (March 2008), available at http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf.

34 See Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation* (June 2009), available at http://www.cabinetoffice.gov.uk/media/216734/nss2009v2.pdf.

35 See the UK's 2008 National Security Strategy, supra note 33 at pp. 10–11 and pp. 25 and 28, and its 2009 National Security Strategy, ibid. at pp. 75–83.

36 See HM Government, *Pursue, Prevent, Protect, Prepare: The United Kingdom's Strategy for Countering International Terrorism* (March 2009), available at http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/news-publications/publication-search/contest/contest-strategy/contest-strategy-2009?view=Binary.

37 See p. 4 of HM Government, *Pursue, Prevent, Protect, Prepare: The United Kingdom's Strategy for Countering International Terrorism – Annual Report* (March 2010), available at http://www.statewatch.org/news/2010/apr/uk-nss-contest-annual-report-2010.pdf.

The CONTEST strategy consists of four components: **(1) Prevent**, which attempts to reduce the threat of international terrorism by focusing on the radicalization of individuals. This includes fixing structural problems, deterring those who incite and organize terrorism, and waging a campaign to counter ideologies that are brandished in support of terrorism strategy; **(2) Pursue**, which tries to investigate and stop terrorists posing a threat to the UK and its interests through intelligence collection and analysis, and disruption (especially through prosecutions); **(3) Protect**, which focuses on improving overall security, including with regard to borders, certain utilities, transportation, and public places; and **(4) Prepare**, which conducts risk and vulnerability analysis and preparedness evaluation, in order to develop improved response capabilities to terrorist threats.

Although all four aspects of the CONTEST strategy have a role to play in deterring or combating home-grown terrorism, the Prevent arm of the strategy has garnered the most attention in this regard. In 2009, the UK published its most recent guide for local partners (i.e., police and local government associations) regarding how to implement the prevent portion of the contest strategy, which includes tips on how to locate radicals and strategies to employ in order to encounter radicalization.[38] The Prevent strategy has five objectives:

- to challenge the ideology behind violent extremism and support mainstream voices;
- disrupt those who promote violent extremism and support the places where they operate;
- support individuals who are vulnerable to recruitment or who have already been recruited by violent extremists;
- increase the resilience of communities to violent extremism; and
- address the grievances which ideologues are exploiting.[39]

Some of the mechanisms used by the UK government to address these objectives include:

- giving financial and other support to communities, organizations and institutions that challenge the messages of those violent extremists who misrepresent the Islamic faith and put lives in danger;
- working with local residents and groups in vulnerable areas to identify people or groups known for promoting violent extremism;
- providing safe places for debate; and
- assisting local organizations to identify and research the grievances expressed by people drawn to extremism.[40]

---

38 See HM Government, *Delivering the Prevent Strategy: An Updated Guide for Local Partners* (August 2009), available at http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/news-publications/publication-search/prevent/prevent-guide-partners?view=Binary.

39 Ibid. at p. 6.

40 For a fuller explanation of the exact steps taken by the UK government and its local partners to put these mechanisms in place, see supra note 38.

CANADA

PREPARED FOR THE SPECIAL SENATE COMMITTEE ON ANTI-TERRORISM

RECENT DEVELOPMENTS IN ANTI-TERRORISM LAW AND POLICY IN THE UNITED STATES

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

5 August 2010

INTRODUCTION

This paper provides an overview of some of the recent developments in anti-terrorism law and policy in the United States. It outlines the legislative framework that the United States has put into place to combat and prevent terrorism, and highlights some of the recent case law developments regarding the terrorism provisions contained in various U.S. statutes. The paper also provides an update on some of the recent policy initiatives the United States has put into place to deter homegrown terrorism, as well as a summary of various studies conducted in the United States on that topic.

LEGISLATIVE FRAMEWORK AND RELEVANT CASE LAW

The United States has passed many laws since the events of 11 September 2001 that deal directly or tangentially with terrorism. However, a summary of all of the laws passed relating to terrorism or terrorist activity in the United States since that time is beyond the scope of this paper, particularly because unlike Canada or the United Kingdom, criminal law is primarily a state responsibility in the United States, and accordingly, criminal laws dealing with terrorism will necessarily vary from state to state.

In addition, it is somewhat difficult to track the progress and all changes made to federal laws concerning terrorism in the United States, because again unlike Canada and the United Kingdom, where statutes generally stand alone unless their sole function is to amend pre-existing pieces of legislation, all federal legislation in the United States, once enacted, becomes integrated into the United States Code (U.S.C.),[1] which is the codification by subject matter of the general and permanent federal laws of the United States. The section numbers of the provisions contained in the original enactments are not preserved, once the material has been integrated into to the U.S.C., and it therefore becomes challenging to determine the provenance of a particular section of this Code.

Having said all of the above, the primary legislative instrument used by the United States at the federal level to combat terrorism remains the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, also known as the USA PATRIOT Act (the Patriot Act).[2] This section of the paper will therefore mainly focus on six key subject matter areas contained in that Act:

- new crimes and penalties;
- new investigative tools and procedures;
- electronic surveillance and communications interception;
- information gathering, secrecy and sharing;

---

1 Federal Alcove: Reserve. The U.S.C. is divided by broad subject into 50 titles. Title 18 of the U.S.C. deals with crimes and criminal procedure, and Chapter 113B of that title deals with terrorism.

2 P.L. 107-56, 115 Stat. 272 (2001).

- the listing of terrorist entities; and
- the suppression of terrorist financing.

This paper will not discuss the evolution, in U.S. law, of the legislative provisions governing the detention and trial of individuals initially referred to as "unlawful enemy combatants," at the U.S. military base at Guantanamo Bay, Cuba. The continued detention and many of the trials of these individuals are governed by legislative instruments other than the Patriot Act, such as the *Military Commissions Act of 2006*[3] and the *Military Commissions Act of 2009*.[4]

A. New Crimes and Penalties

In contrast to the situation in Canada, where no definition of "terrorist activity" existed in the *Criminal Code*[5] before the *Anti-terrorism Act*[6] came into force, the U.S.C. contained both a definition of "international terrorism"[7] and a specific chapter dealing with terrorism and terrorist offences (Chapter 113B or the Terrorist Chapter) before the Patriot Act was enacted. However, the Patriot Act added a definition of "domestic terrorism" to the U.S.C. It also broadened what constitutes a "federal crime of terrorism" under U.S. law. A "federal crime of terrorism" is generally some type of violent predicate offence,[8] such as homicide, attempted homicide or a bombing, committed in circumstances "calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct."[9] Like the *Anti-terrorism Act* in relation to Canada or the United Kingdom, in relation to its own six main terrorism statutes, the Patriot Act introduced several new offences into U.S. law. However, many of these new offences seem designed to capture the activities of terrorists and non-terrorists alike. They are not, in other words, specifically or exclusively designed to capture terrorist activities or the actions of terrorist groups, although terrorists may be more likely to commit them than non-terrorists. For example, section 801 of the Patriot Act modifies section 1993 of Title 18 of the U.S.C. by making it an offence to commit acts of violence against mass

---

3 P.L. 109-366, 120 Stat. 2600 (2006).

4 P.L. 111-84, 123 Stat. 2199 (2009).

5 R.S.C. 1985, c. C-46.

6 S.C. 2001, c. 41.

7 Prior to the coming into force of the Patriot Act, section 2331, Chapter 113B, Title 18 of the U.S.C. essentially defined international terrorism as an activity, occurring primarily outside of the United States or transcending national boundaries in terms of the means employed, targets of the action or location in which the perpetrators operate or seek asylum, which involves acts of violence that are dangerous to human life and would be crimes under state or federal law, that appear to be intended to intimidate or coerce a civilian population, influence the policy of government by intimidation or coercion or to affect the conduct of a government by assassination or kidnapping.

8 A predicate offence is an offence that the prosecution will have to prove the accused person committed, in order to convict that person of a second offence. The second offence is generally more serious than the predicate offence and carries with it more substantial penalties. For examples in the Canadian context, see *R.* v. *Creighton*, [1993] 3 S.C.R. 3; and *R.* v. *Gosset*, [1993] 3 S.C.R. 76.

9 See section 2332b of Chapter 113B, Title 18 of the U.S.C.

transportation systems, while section 817 of the Patriot Act modifies Title 18 of the U.S.C. by making it an offence, under section 175b of the Code, for convicted felons, illegal aliens, and fugitives to possess biological toxins or weapons.

It would appear from a document released last year by the Centre on Law and Security, New York University School of Law,[10] that the new crimes and penalties related to terrorism that were introduced by the Patriot Act have been used considerably since 11 September 2001. This document indicates that as of 25 September 2009, the U.S. Department of Justice had indicted 828 defendants on charges associated with terrorism. At that time, 235 trials were still pending, leaving 593 resolved indictments. Of those 593 indictments, 523 had resulted in a conviction, either at trial or as a result of a guilty plea.[11]

B. New Investigative Tools and Procedures

Prior to the events of 11 September 2001, prosecutors and law enforcement officials had two significant tools available to assist them in investigating crimes: the grand jury process and material witness arrest provisions. Both could result in a person being summoned to answer questions regarding a criminal offence, without necessarily being charged with an offence. However, the Patriot Act introduced certain changes to the grand jury process, and the events of 11 September 2001 appear to have changed how the material witness arrest process is being used. Both of these changes have proven to be controversial.

The purpose of the federal grand jury in the United States is to determine whether or not an individual has committed an offence, and if so, to indict him or her.[12] As an inquisitorial or investigatory body, the grand jury does not require probable cause or any other threshold of proof before summoning a witness. The grand jury need only believe that the person in question has information relevant to the matter being investigated. Persons subpoenaed to testify before a grand jury who refuse to appear or who appear but refuse to answer questions may be held in contempt, unless they can prove privilege. They can similarly be held in contempt if they are required to bring relevant documents or property with them and fail to do so, unless they claim privilege and can prove it. While a person who appears before a grand jury can refuse to answer questions on the grounds that the answers might incriminate him or her, the grand jury can often get at the information another way, by subpoenaing a third-party witness to testify or subpoenaing the custodian of a document to produce it. There is no specific statutory right to counsel in the grand jury process, as the 6th Amendment constitutional right to counsel takes effect only once someone has been indicted for a crime. The only people who strictly have the right to attend a grand jury hearing are the jury members, the Department of Justice lawyer, the person being examined, a court reporter,

---

10 Centre on Law and Security, New York University School of Law, *Highlights from the Terrorist Trial Report Card 2001–2009: Lessons Learned*, Centre for Law and Security, New York, 2009, available online at http://www.lawandsecurity.org/publications/TTRCHighlightsSept25th.pdf.

11 Ibid., p. 2.

12 The rules governing the federal grand jury process in the United States are found in Chapter 215, Title 18 of the U.S.C. and in Part III of the Federal Rules of Criminal Procedure (2006) (F.R.Crim.P.).

and, if necessary, interpreters.[13] In the federal grand jury process, witnesses may bring lawyers with them to the grand jury hearing; however, the lawyers are not allowed into the grand jury room to listen to the proceedings. Witnesses wishing to consult with counsel during the proceedings must ask for, and obtain, permission to exit the room to do so.

Prior to the enactment of the Patriot Act, information obtained through a grand jury inquiry was generally kept secret. It could be disclosed only by the Department of Justice or others assisting in the grand jury process to enforce the criminal law (for example, to lay charges against someone).[14] However, section 203(a) of the Patriot Act altered the grand jury process. Section 203(a) allows information obtained during a grand jury hearing related to intelligence, counterintelligence[15] or foreign intelligence to be released to a wide variety of federal officials to assist them in the performance of their duties.[16] Although section 203(a) introduces a notification safeguard, requiring courts to be confidentially notified when disclosure has been granted to such federal officials,[17] this safeguard stops far short of requiring prior court approval before releasing the information, which was the norm before the enactment of the Patriot Act. Accordingly, some have been critical of this section 203(a), claiming that it raises privacy concerns and can be easily abused by government officials.

With respect to the material witness arrest process,[18] it can be used by federal law enforcement officials to arrest a witness in order to secure his or her testimony in a criminal proceeding.[19] A warrant is required before the individual can be arrested. To obtain an arrest warrant, the Department of Justice must file an application with a federal district court and establish to the court's satisfaction that the person in question has information material to a criminal proceeding and that it is impracticable to ensure the person's presence in any other way.[20] Because it can be used to investigate any offence, not just terrorist offences, the material witness arrest process in the United States has an extremely wide application.

A person arrested under the material witness arrest process must be brought before a judge for a detention review as soon as possible. The judge will decide whether or not to release this person or to continue his or her detention.[21] There is a judicial presumption in favour of release, unless there is probable cause to believe the person has committed certain

---

13 F.R.Crim.P. 6(d)(1).

14 F.R.Crim.P. 6(e). For a thorough discussion of the grand jury process as it existed before the coming into force of the Patriot Act, as well as a discussion of the dangers presented by the amendments to the process introduced by section 203(a) of the Patriot Act, please refer to Sara Beale and James Felman, "The Consequences of Enlisting Federal Grand Juries in the War on Terrorism: Assessing the Patriot Act's Changes in Grand Jury Secrecy," *Harvard Journal of Law and Public Policy*, Vol. 25, 2002, p. 699.

15 Under the Patriot Act, foreign intelligence and counterintelligence are broadly defined terms.

16 F.R.Crim.P. 6(e)(3)(D).

17 F.R.Crim.P. 6(e)(3)(D)(ii).

18 The provisions governing the material witness arrest process can be found in Chapter 207, Title 18 of the U.S.C.

19 Under U.S. law, a criminal proceeding includes a grand jury proceeding.

20 18 U.S.C. 3144.

21 18 U.S.C. 3142.

types of serious federal offences, one of which is the federal crime of terrorism.[22] If the person is released, the judge may impose conditions on the release.[23] There is no set time limit for the detention of a material witness. If the judge affirms the continued detention of the individual, he or she may be held as long as his or her testimony is needed for criminal proceedings, which could mean detention until a trial is completed.

In terms of changes in how the material witness arrest process has been used after 9/11, approximately 70 individuals, primarily Muslim men, were detained since that date so as to facilitate the investigation of terrorist crimes. The American Civil Liberties Union (ACLU) and Human Rights Watch have argued that most of these individuals were arrested on thin or spurious grounds, and that their arrests and detentions have not generally led to charges being laid against them or anyone else.[24]

C. Electronic Surveillance and Communications Interception

U.S. legislation had tiers of privacy protection requirements when it came to electronic surveillance prior to the enactment of the Patriot Act. While prior judicial authorization or at least some sort of warrant or subpoena was generally required before surveillance or interception, the stringency of the test for obtaining prior permission depended on the type of information being collected, the reasonable expectation of privacy attached to the information and the reason why the law enforcement or government official was seeking it (in other words, whether it was being sought for foreign intelligence or other purposes).

However, the Patriot Act amended U.S. law to broaden the capacity of law enforcement officials to obtain certain types of court orders for electronic surveillance or communications interception. It has also amended the law to broaden the types of information that may be obtained under such orders in certain circumstances.

For example, section 206 of the Patriot Act allows for roving FISA (*Foreign Intelligence Surveillance Act*)[25] orders. These orders, which must be obtained from the FISA court, need not specifically identify the particular instrument of surveillance, facilities or place where the surveillance is to occur. Rather than intelligence officials needing to obtain a separate FISA order for every telephone or device they wish to tap, this provision allows them to obtain a global order permitting them to tap multiple devices belonging to a single individual. In other words, it allows them to target a person, rather than a specific phone. In order to obtain a roving FISA order under section 206, the court must be satisfied that the target is a "foreign power" as defined in section 1801 of Title 50 of the U.S.C. and that the actions of the target may have the effect of thwarting surveillance.[26]

---

22 18 U.S.C. 3142(a), (b), (e) and (f).

23 18 U.S.C. 3142(c).

24 See the 27 June 2005 article entitled "Scores of Muslim Men Jailed Without Charge: Justice Department Misused Material Witness Law in Counterterrorism Efforts," located on the Human Rights Watch website at http://hrw.org/english/docs/2005/06/27/usdom11213.htm. Also, see the report entitled *Witness to Abuse: Human Rights Abuses under the Material Witness Law since September 11*, published online by Human Rights Watch and the ACLU on 26 June 2005, and available at http://www.hrw.org/en/reports/2005/06/26/witness-abuse-0.

25 See 50 U.S.C., Chapter 36, which contains FISA.

26 50 U.S.C. 1805(c)(2)(D) and 1805(d).

Another example is section 218 of the Patriot Act, which allows federal officials to apply for FISA surveillance orders when gathering foreign intelligence is a *significant* reason for the order rather than *the* reason, which was the case prior to the enactment of the Patriot Act.[27] Arguably, this means that FISA orders could be used in criminal investigations, as long as they have a foreign intelligence aspect to them. This is potentially problematic because the test one has to meet in order to get a FISA order is generally less stringent than the test one has to meet to obtain a Title III order (the type of surveillance order generally required when one is investigating a serious crime).

The United States also did away with the need for prior judicial authorization for electronic surveillance in certain circumstances, from a period commencing shortly after 11 September 2001 until sometime in January of 2007, when, due to political pressures placed on the U.S. government by civil liberties groups, the U.S. Congress and others, the warrantless surveillance program was cancelled.

Details regarding the U.S. warrantless surveillance program first began to come to light on 16 December 2005, when *The New York Times* published an article that claimed that President Bush had signed a secret Executive Order in 2002, authorizing the National Security Agency (NSA), which gathers foreign signals intelligence for the United States, to monitor and intercept international telephone calls and emails made by persons within the United States to persons outside of the United States or vice versa, without the need to obtain prior judicial authorization from the FISA court.[28] This program became commonly known as the Terrorist Surveillance Program (TSP). Following the release of this 2005 article, President Bush confirmed that he had, in fact, signed such an order, creating the TSP.[29] He and his advisors asserted that the President had the requisite authority to issue such an order based on his powers under Article II of the U.S. Constitution[30] and on a joint congressional resolution originating in the Senate, S.J. Res. 23, cited as the *Authorization for Use of Military Force* (AUMF) resolution,[31] which was signed into law by President Bush on 18 September 2001.[32] The AUMF resolution authorized the President to use "all necessary and appropriate force against those nations, organizations, or persons he determines planned,

---

27 See, for example, 50 U.S.C. 1804(a)(7)(B).

28 E. Lichtblau and J. Risen, "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times*, 16 December 2005, p. 1.

29 D. E. Sanger, "In Address, Bush Says He Ordered Domestic Spying," *The New York Times*, 18 December 2005, p. 1.

30 This article outlines the President's executive powers, including his powers as Commander in Chief of the Armed Forces.

31 See the White House, "President's Radio Address," 17 December 2005, available online at http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html; the White House, "Press Briefing by Attorney General Alberto Gonzales and General Michael V. Hayden, Principal Deputy Director of National Intelligence," Press release, 19 December 2005, available online at http://www.globalsecurity.org/intell/library/news/2005/intell-051219-dni01.htm; and Assistant Attorney General William Moschella, Letter to the leaders of the Senate and House of Representatives Intelligence Committees, 22 December 2005, available online at http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf.

32 P.L. 107-40, 115 Stat. 224 (2001).

authorized, committed or aided" the 11 September 2001 terrorist attacks, or harboured those that did so, for the purpose of preventing "future acts of terrorism against the United States" by these nations, individuals or organizations.[33]

In the wake of these revelations, various persons and organizations began expressing concern that President Bush may not have had the necessary constitutional and/or congressional authority to issue his 2002 Executive Order. They also expressed concern that the warrantless electronic surveillance conducted by the NSA pursuant to the Order to date may have violated the 4th Amendment rights (protection from unreasonable search and seizure) of U.S. persons.[34] Questions began to emerge about the government's assertion that the President's Executive Order was necessary because periods of warrantless surveillance (longer than those permissible under FISA) are necessary to prevent and combat terrorism.[35] These concerns and questions, in turn, prompted certain civil liberties organizations, such as the ACLU and the Centre for Constitutional Rights (CCR) to file lawsuits against the U.S. government, challenging the legality of the TSP, claiming that the TSP not only violated the 4th Amendment rights of those living in the United States, but also their 1st Amendment (freedom of speech) rights. Various U.S. congressional committees, most notably, the U.S. Senate Judiciary Committee, also began to hold hearings to investigate the legality of the program. In the wake of all of this controversy, on 17 January 2007, then U.S. Attorney General, Alberto Gonzales, announced, in a letter to Congress, that the government would be cancelling the TSP, and would no longer be authorizing warrantless wiretapping under authority of executive order, and would instead be conducting electronic surveillance in accordance with FISA. He also indicated that the government would be seeking to amend FISA to provide a specific statutory basis for the

---

33 For more information on the AUMF resolution, please see Richard F. Grimmett, *Authorization For Use Of Military Force in Response to the 9/11 Attacks (P.L. 107-40): Legislative History*, Congressional Research Service, Washington, D.C., 4 January 2006, available on the Federation of American Scientists' website at http://www.fas.org/sgp/crs/natsec/RS22357.pdf.

34 See, for example, the comprehensive legal analysis of these matters contained in Elizabeth Bazan and Jennifer Elsea, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, Memorandum, Congressional Research Service, Washington, D.C., 5 January 2006, available on the Federation of American Scientists' website at http://www.fas.org/sgp/crs/intel/m010506.pdf. See, as well, M. H. Halperin, *A Legal Analysis of the NSA Warrantless Surveillance Program*, 5 January 2006, available on the Centre for American Progress website at http://www.americanprogress.org/atf/cf/{E9245FE4-9A2B-43C7-A521-5D6FF2E06E03}/nsa_surveillance.pdf.

35 While government agencies are generally required to obtain prior authorization from the FISA court before engaging in warrantless surveillance, FISA does contain exceptions to the court order requirement. For example, the Attorney General can order electronic surveillance of certain foreign powers without a court order for up to one year (50 U.S.C. 1802), electronic surveillance without a court order in emergency situations for up to 72 hours, while an order approving such surveillance is sought from the FISA court (50 U.S.C. 1805(f)), and electronic surveillance without a court order for 15 days following a declaration of war by Congress (50 U.S.C. 1811).

TSP.[36] Subsequently, on 5 August 2007, Congress enacted the *Protect America Act of 2007*,[37] which, among other things:

- amended FISA to state that nothing under its definition of "electronic surveillance" shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States;

- allowed the Director of National Intelligence (DNI) and the Attorney General (AG), for periods up to one year, to authorize the acquisition of foreign intelligence information, either inside or outside of the United States as long as the ultimate target of the surveillance was outside the United States, and the following criteria were also met: (1) a significant purpose for acquiring information through surveillance was to obtain foreign intelligence information (2) reasonable procedures were in place for determining that such acquisition concerned persons outside the United States (the FISA court was limited to an accept or reject power in relation to these procedures); (3) the acquisition involves obtaining foreign intelligence information from or with the assistance of a communication service provider or other person who has access to communications; and (4) minimization procedures, which satisfied the definition of minimization procedures under FISA, were in place to ensure the smallest level of privacy intrusion while obtaining information (the FISA court had authority to determine whether or not the minimization procedures were adequate).

In addition, the AG was required to report to the FISA Court the procedures by which the government determined that such acquisitions did not constitute electronic surveillance directed at someone inside the United States. He or she was also required to report to the congressional intelligence and judiciary committees semi-annually concerning acquisitions made during the previous six-month period.

Most of the Act's provisions were subject to sunset clauses which would serve to terminate them 180 days after the enactment of the statute, although authorizations for the acquisition of information made in accordance with the Act, and directives issued pursuant to such authorizations, would remain effective until their particular expiration dates.

Following the enactment of the *Protect America Act of 2007*, numerous lawsuits challenging the constitutional validity of this new statute were also initiated, and on 18 July 2008, Congress enacted the *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008* (FISA Amendments Act of 2008),[38] which essentially replaced the provisions contained in the *Protect America Act of 2007*, and increased, to a certain degree, FISA court supervision of electronic surveillance initiatives authorized by the DNI and the AG. For example, the FISA Amendments Act of 2008 expressly states that the surveillance may not intentionally target any person known at the time of acquisition to be located in the United States, may

---

36 The text of former Attorney General Alberto Gonzales' 17 January 2007 letter to Congress is available at http://www.fas.org/irp/congress/2007_cr/fisa011707.html.

37 P.L. 110-55, 121 Stat. 552 (2007). The text of this Act is available online at http://www.justice.gov/archive/ll/docs/text-of-paa.pdf.

38 P.L. 110-261, 122 Stat. 2463 (2008). The text of this Act is available online at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ261.110.pdf.

not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States, and may not intentionally target a U.S. person reasonably believed to be located outside the United States. In addition, although there are exceptions for exigent circumstances, before the DNI and AG authorize the targeting of foreign persons abroad under the Act, they must first obtain a FISA Court order, approving the authorization. Another significant change introduced by the FISA Amendments Act of 2008 is that it contains provisions providing retroactive immunity for telecommunications providers who assisted the U.S. Government under the TSP in existence between September of 2001 and January of 2007.[39]

Notwithstanding improvements introduced by the FISA Amendments Act of 2008, lawsuits appear to be continuing against both telecommunications providers who assisted the NSA under the TSP. Lawsuits have also been initiated challenging the constitutional validity of the new Act itself.[40] The provisions of the FISA Amendments Act of 2008 will expire in 2012, unless re-extended by Congress.

D. Information Gathering, Secrecy and Sharing

Most of the amendments introduced by the Patriot Act respecting information gathering, secrecy and sharing seem less concerned with information secrecy and more concerned with giving government officials more power to gather foreign intelligence information from a variety of sources and share it with other government officials and agencies.[41]

For example, section 203(b) of the Patriot Act allows law enforcement officials to share foreign intelligence information, obtained through a legally authorized wiretap, with a wide array of federal officials, as long as it is shared for official use, while section 203(d) of the Patriot Act allows law enforcement officials to share foreign intelligence information

---

39 For more specific information regarding the provisions in the FISA Amendments Act of 2008 that provide retroactive immunity for telecommunications providers, please see Edward C. Liu, *Retroactive Immunity Provided by the FISA Amendments Act of 2008*, Congressional Research Service, Washington, D.C., 25 July 2008, available on the Federation of American Scientists' website at http://www.fas.org/sgp/crs/intel/RL34600.pdf.

40 Ibid. Also see Julian Sanchez, "ACLU, EFF challenge constitutionality of FISA amendments," 19 October 2008, available online at http://arstechnica.com/tech-policy/news/2008/10/aclu-eff-challenge-constitutionality-of-fisa-amendments.ars; the EFF News release, "EFF and ACLU Planning to Appeal Dismissal of Dozens of Spying Cases," 3 June 2009, available online at http://www.eff.org/press/archives/2009/06/03; and Nick Divito, "ACLU Sues to See Fed E-mail Spying Records," *Courthouse News Service*, 3 June 2010, available online at http://www.courthousenews.com/2010/06/03/27810.htm.

41 Having said this, some sections of the Patriot Act are concerned with information secrecy. One example is section 213, the controversial "sneak and peak" warrant provision. Section 213 allows law enforcement officers to secretly enter a place to conduct a search, either physically or virtually, without providing prior notification to the person whose property they will be searching. A court may issue a "sneak and peak" warrant if it is satisfied that there are reasonable grounds to believe that prior notification would risk destroying evidence, result in bodily injury, jeopardize an investigation or delay a trial (18 U.S.C. 2075). While the person whose premises and property are searched is required to be notified of the search after the fact, notification may be delayed for a "reasonable" time. What constitutes a reasonable time is not defined in the U.S.C. or the Patriot Act.

discovered in the course of a federal criminal investigation with the intelligence community, notwithstanding any other provision of law.

Another example of increased information gathering and sharing powers introduced by the Patriot Act is section 215, which allows foreign intelligence officials to obtain access to "tangible items" under FISA (tangible items may include a wide array of records or documents, regardless of who is in possession of them) through an *ex parte* order of the FISA court. The FISA court will issue such an order only if the official requesting it is engaged in a foreign intelligence investigation conducted to protect against international terrorism or clandestine intelligence activities. Prior to the enactment of the Patriot Act, foreign intelligence officials could obtain these types of FISA orders only in relation to vehicle rental, transportation, storage rental and housing accommodation records.

Section 215 of the Patriot Act has proven to be a controversial provision in both the United States and Canada. Canada's Privacy Commissioner and British Columbia's Information and Privacy Commissioner have both expressed concerns that section 215 could allow U.S. intelligence agencies to obtain personal information about Canadians from U.S. companies with offices in Canada, or from U.S. companies in the United States who hold personal information of Canadians due to outsourcing contracts.[42]

Yet another example of increased information gathering and sharing powers provided to federal intelligence authorities under the Patriot Act can be found in sections 358 and 505 of that Act, which grant the FBI the authority to compel communications firms, such as Internet service providers or telephone companies, and financial institutions, such as banks or credit unions, as well as other third parties, to produce certain customer or financial data whenever the FBI certifies that the records are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.[43] The FBI can compel production merely by issuing a letter known as a National Security Letter (NSL). No prior judicial authorization is required. Companies that receive NSLs are prohibited from ever revealing to anyone that they received such a letter.

Initially, it appeared that the courts were going to rule that NSLs themselves were unconstitutional. Two U.S. District Federal Court decisions, one issued in 2004, in which the Court held that section 505 violated the 1st (freedom of speech) and 4th (protection from unreasonable search and seizure) Amendments of the U.S. Constitution, and another

---

42 See, for example, the report of the Information and Privacy Commissioner of British Columbia entitled *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*, October 2004, available online at http://oipc.bc.ca/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final.pdf. Chapters 6 and 10 provide a discussion of the potential impact of section 215 of the Patriot Act on Canadians. See, as well, the submission made by the Office of the Privacy Commissioner of Canada to the Information and Privacy Commissioner of British Columbia dated 18 August 2004, entitled *Transferring Personal Information about Canadians Across Borders – Implications of the* USA PATRIOT Act, which is available online at http://www.privcom.gc.ca/media/nr-c/2004/sub_usapa_040818_e.pdf.

43 See 18 U.S.C. 2709.

issued in 2005, in which the Court held that the automatic gag order under section 505,[44] which prohibits third parties from disclosing that they have received an NSL, violated the 1st Amendment,[45] seemed to support this position, However, the government filed an appeal of both decisions, and on 15 December 2008, the U.S. Court of Appeals for the Second Circuit ruled that the NSLs were constitutional. It found, however, that the parts of the statute that placed the burden on NSL recipients to initiate judicial review of the gag order were invalid, and that the onus should instead be on the government to justify the gag order.[46] Both the government and Doe cross-appealed, and this further appeal resulted in the gag order issued in this particular case being upheld.[47]

Accordingly, it would appear that while the government now has the burden of justifying gag orders with respect to NSLs, the FBI can continue to issue both NSLs themselves, as well as gag orders, as long as the FBI provides appropriate justification for the latter.

E. Listing of Terrorist Entities

While a process for listing terrorist entities was introduced into U.S. law following 11 September 2010, it was not introduced in the Patriot Act, but by means of an Executive Order, E.O. 13224, signed by the President.[48] As a consequence, the listing process is somewhat less formal under U.S. law than under Canadian law. As is the case in Canada, being a listed or designated an individual or entity under E.O. 13224 is not, in and of itself, an offence. However, E.O. 13224 does prohibit U.S. persons and persons within the United States from dealing with, or engaging in, transactions involving the property of listed individuals or entities and from making or receiving any contribution of funds, goods or services to or for the benefit of listed individuals or entities. It also prohibits any attempt to evade a blocking order made by the Office of Foreign Asset

---

44 *Doe* v. *Ashcroft*, 334 F. Supp. 2d 471 (S.D. New York 2004).

45 *Doe* v. *Gonzales*, 386 F. Supp. 2d 66 (Connecticut 2005).

46 *Doe* v. *Musakey*, 549 F.3D 861 (2ND CIR. 2008).

47 *Doe* v. *Holder*, 665 F. Supp. 2d 426 (2009).

48 E.O. 13224 empowers the Secretary of State or the Secretary of the Treasury, in consultation with each other and with the Attorney General, to place individuals or entities on a list if the Secretaries are satisfied that the individuals or entities are (a) foreign individuals or entities determined to have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy or economy of the United States, (b) individuals or entities that are owned or controlled by those who have committed acts of terrorism or pose a significant risk of committing such acts, or (c) those who assist in, sponsor or provide financial, material or technological support for, or financial or other services to or in support of, such acts of terrorism or to entities or individuals already on the list. The full text of E.O. 13224 is available online at http://www.fas.org/irp/offdocs/eo/eo-13224.htm.

Control (OFAC) of the Department of the Treasury.[49] Those who violate the prohibitions contained in E.O. 13224 may be subject to civil or criminal penalties.[50]

[49] OFAC is empowered to take action to block the assets of a listed individual or entity in the United States or in possession or control of U.S. persons. It may also notify U.S. financial institutions of the blocking order, and direct them to block the assets of the listed individual or entity.

[50] Those who violate the prohibitions in E.O. 13224 may be sentenced to up to 10 years' imprisonment or a fine of $500,000 for corporations and $250,000 for individuals, or both.

F. Suppression of Terrorist Financing

The Patriot Act introduced new forfeiture provisions specifically related to terrorism.[51] However, it did not introduce new offences designed to discourage, deter or prohibit people from dealing with terrorist property. This is likely because the offences of providing material support to terrorists or terrorist organizations already existed under U.S. law prior to the enactment of the Patriot Act.[52] Similarly, the definition of money laundering under U.S. law prior to the enactment of the Patriot Act was broad enough to encompass terrorist activity,[53] and thus, there was no need to introduce amendments through the Patriot Act to make the existing U.S. legislative scheme dealing with money laundering specifically applicable to terrorist financing offences. The Patriot Act was used, however, to strengthen reporting requirements imposed on financial institutions, stiffen penalties imposed on institutions for failure to comply with reporting requirements, and promote information sharing between financial institutions and law enforcement agencies.[54]

SUNSET PROVISIONS AND THE PATRIOT ACT

In contrast to the *Anti-terrorism Act*, the Patriot Act contained no provision requiring Congress to undertake a comprehensive review of that statute. It did, however, as originally enacted, contain 16 provisions subject to sunset clauses. All of these provisions were scheduled to sunset on 31 December 2005 unless reauthorized by Congress. Some of the provisions that were originally scheduled to sunset on that date have been discussed above, including sections 203(b) (sharing wiretap information), 203(d) (sharing foreign intelligence information), 206 (roving FISA wiretaps), 215 (access to tangible items under FISA), and 218 (significant purpose for FISA orders). As a result of these sunset provisions, the House of Representatives and the Senate conducted reviews of the Patriot Act to see whether reauthorization of some or all of the sunsetted provisions was warranted. At the same time, although no such review was mandated by the Act, they examined the Act as a whole, to see whether any changes, in terms of procedural protections available to those affected by the provisions, were warranted. The committees most involved in this review were the Senate Judiciary Committee and the U.S. House of Representatives Committee on the Judiciary (the House Judiciary Committee). Following study by these committees, the House of Representatives and the Senate each introduced its own reauthorization

---

51 See, for example, sections 106 and 806 of the Patriot Act.

52 See 18 U.S.C. 2339A and 2339B, which contain the offences of knowingly providing material support or resources to terrorists or terrorist organizations, respectively. Section 805 of the Patriot Act did, however, amend section 2339A slightly by prohibiting the provision of expert advice or assistance to terrorists. Sections 2339A and 2339B were further modified by section 6603 of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA). These latter amendments, among other things, made the definitions of "material support or resources," "training," and "expert advice and assistance," as used in these provisions, more precise. The U.S. Supreme Court recently upheld the constitutionality of 2339B in *Holder* v. *Humanitarian Law Project*, No. 08-1498, United States Supreme Court, 21 June 2010. This case is available online at http://www.supremecourt.gov/opinions/09pdf/08-1498.pdf.

53 See 31 U.S.C. 5340(2).

54 See, for example, sections 311, 312, 314, 321, 351, 352, 356, 361 and 362 of the Patriot Act.

bill.[55] After two short extensions of all Patriot Act provisions scheduled to sunset on 31 December 2005,[56] a conference committee report[57] that attempted to reconcile differences between the House and Senate bills, and much debate, Congress eventually passed H.R. 3199, the *USA PATRIOT Improvement and Reauthorization Act of 2005* (the Patriot Reauthorization Act or PRA).[58] At approximately the same time, Congress passed another bill, S. 2271, the *USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006* (the Additional Reauthorizing Amendments Act or ARAA).[59] Both bills were signed into law by the President on 9 March 2006. Under these Acts, 14 of the 16 provisions originally scheduled to sunset on 31 December 2005 were made permanent. Only two provisions, destined to sunset were not made permanent: section 206, which allows for roving FISA wiretaps, and section 215, which allows foreign intelligence officials to obtain access to tangible items under FISA through ex parte orders of the FISA court. The expiry dates for these provisions were, however, extended to 31 December 2009.[60] In addition, these two Acts served to enhance some of the procedural protections available to those who might be impacted by these two provisions. The validity of these two provisions has since been extended to 28 February 2011.

---

55 The bill initially introduced by the House of Representatives was H.R. 3199, originally entitled the USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005. The bill initially introduced by the Senate was S. 1389, entitled the USA PATRIOT Improvement and Reauthorization Act of 2005. For a thorough overview of the initial versions of H.R. 3199 and S. 1389 and the differences between them, please see Charles Doyle, *USA PATRIOT Act: Background and Comparison of House- and Senate-approved Reauthorization and Related Legislative Action*, Congressional Research Service, Washington, D.C., 9 August 2005, available on the Federation of American Scientists' website at http://www.fas.org/sgp/crs/intel/RL33027.pdf.

56 On 30 December 2005, the President signed into law *An Act to amend the USA PATRIOT ACT to extend the sunset of certain provisions of that Act and the lone wolf provision of the Intelligence Reform and Terrorism Prevention Act of 2004 to 1 July 2006*, P.L. 109-160, 119 Stat. 2957. Despite its name, the Act extended the provisions in the Patriot Act destined to sunset and the "lone wolf" provision in the IRTPA only to 3 February 2006. Subsequently, on 3 February 2006, the President signed *An Act to amend the USA PATRIOT ACT to extend the sunset of certain provisions of such Act*, P.L. 109-170, 120 Stat. 3. This statute extended the validity of these same provisions to 10 March 2006.

57 In the United States, a bill cannot become law unless it is passed in identical form by both Houses of Congress. Once the Senate amends and agrees to a House of Representatives bill or vice versa, the two Houses may begin to resolve their differences by way of a conference committee consisting of members chosen by both Houses that will attempt to arrive at a compromise between differing versions of the bill, or through an exchange of amendments between Houses. The conference committee report respecting bills H.R. 3199 and S. 1389 can be obtained by searching the Library of Congress' website at http://thomas.loc.gov. For a thorough overview of the version of bill H.R. 3199 produced following the conference committee report, please see Charles Doyle and Brian T. Yeh, *USA PATRIOT Improvement and Reauthorization Act of 2005 (H.R. 3199): A Legal Analysis of the Conference Bill*, Congressional Research Service, Washington, D.C., 17 January 2006, available on the Federation of American Scientists' website at http://www.fas.org/sgp/crs/intel/RL33239.pdf.

58 P.L. 109-177, 120 Stat. 192 (2006). The text of the PRA is available on the Library of Congress' website at http://thomas.loc.gov.

59 P.L. 109-178, 120 Stat. 278 (2006). The text of the ARAA is available on the Library of Congress' website at http://thomas.loc.gov.

60 See section 102 of the PRA.

POLICY INITIATIVES

Just as the United States has numerous statutes at both the federal and state level which attempt to combat terrorism and terrorist activities, it also has undertaken numerous studies and policy initiatives designed to identify or combat the problems associated with homegrown terrorism. A full review of all of these initiatives is beyond the scope of this paper, but below are descriptions of some of the studies and initiatives initiated in the United States on this topic. They have been organized in order of date.

In **June 2006**, former President Bush approved the National Implementation Plan (NIP), the goal of which was to unify and integrate government activities to address the terrorist threat, including the homegrown threat. The NIP integrates diplomatic, homeland security, law enforcement, financial and military as well as intelligence measures.

In **September 2006**, the U.S. Senate Homeland Security and Governmental Affairs Committee began investigating the threat facing the United States from homegrown terrorism and domestic radicalization inspired by violent Islamist extremism. The Committee began its investigation with a hearing looking into radicalization within the Federal prison population. The investigation has continued with a series of hearings examining the root causes of violent domestic radicalization, the tactics and measures used by U.S. law enforcement at every level to prevent and deter homegrown terrorism, the role of the Internet in self radicalization, and general terrorism assessments.

In **April 2007**, Jane Harman introduced a bill in the House of Representatives entitled *Violent Radicalization and Homegrown Terrorism Prevention Act of 2007*.[61] It passed the House of Representatives by a vote of 404–6, but never became law before the end of the 110th Congress. The bill concerned the prevention of "violent radicalization" and "homegrown terrorism,"[62] by establishing the National Commission on the Prevention of Violent Radicalization and Homegrown Terrorism. The Commission would have had to examine and report on facts and causes of violent radicalization, homegrown terrorism, and ideologically based violence in the United States. In addition, the bill would have directed the Secretary of Homeland Security to establish or designate a university-based

---

61 H.R. 1955, 110th Congress (2007–2008).

62 Section 899A of the bill gave the following definitions of "violent radicalization" and "homegrown terrorism":

- "The term 'violent radicalization' means the process of adopting or promoting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change.
- The term 'homegrown terrorism' means the use, planned use, or threatened use, of force or violence by a group or individual born, raised, or based and operating primarily within the United States or any possession of the United States to intimidate or coerce the United States government, the civilian population of the United States, or any segment thereof, in furtherance of political or social objectives."

Center of Excellence for the Study of Violent Radicalization and Homegrown Terrorism in the United States to assist federal, state, and local homeland security officials, through training, education, and research, in preventing violent radicalization and homegrown terrorism in the United States. It would have required the Secretary to conduct a survey of methodologies implemented by foreign nations to prevent violent radicalization and homegrown terrorism and to report to Congress on lessons learned from the survey results.

In **August 2007**, the New York City Police Department issued a comprehensive study of radicalization and the homegrown threat, concluding, "Muslims in the U.S. are more resistant, but not immune, to the radical message."[63] The study examined 11 case studies of individuals and groups that radicalized in the West and identified four stages of radicalization through which initially unremarkable individuals move to the point where they engage in planning or executing a violent attack.[64] The study recommended increased investments in intelligence collection because "the subtle and non-criminal nature of the behaviors involved in the process of radicalization makes it difficult to identify or even monitor them from a law enforcement standpoint."[65]

In **May 2008**, the Senate Homeland Security and Governmental Affairs Committee released a report entitled, "Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat."[66] The Committee concluded that, "despite recognition in the NIP that a comprehensive response is needed, the U.S. government has not developed nor implemented a coordinated outreach and communications strategy to address the homegrown terrorist threat, especially as that threat is amplified by the use of the Internet."[67] In developing a strategy to prevent homegrown terrorism, the Committee directed the federal government to address several key questions including:

- "What, if any, new laws, resources and tactics other than those already employed by intelligence and law enforcement should be used to prevent the spread of the ideology in the United States?
- What should a communications strategy, both on and off the Internet, look like, and what role, if any, should the government have in carrying out that strategy? What role must community and religious leaders play?

---

63 Mitchell D. Silver and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat*, New York City Police Department, New York, 2007, p. 82.

64 For a discussion about the four stages, see Daveed Gartenstein-Ross and Laura Grossman, *Homegrown Terrorists in the U.S. and U.K.: An Empirical Examination of the Radicalization Process*, 2009, p. 21, available at http://www.defenddemocracy.org/downloads/HomegrownTerrorists_USandUK.pdf.

65 Ibid., p. 85.

66 Available on the Committee's website at http://hsgac.senate.gov/public/index.cfm?FuseAction=Home.ViolentIslamistExtremism.

67 Page 15 of the Report.

- What is the purpose of current outreach efforts, and how can those efforts improve, especially with increased coordination at all levels of government?
- What role should local officials and local law enforcement play given their longstanding relationships with the communities they serve and the fact that they are better positioned to recognize and intervene, if and when it is necessary to do so?"[68]

In **April 2009**, the Foundation for Defense of Democracies' Center for Terrorism Research released a Report entitled: *Homegrown Terrorists in the U.S. and U.K.: An Empirical Examination of the Radicalization Process*.[69] The Report examined the radicalization process of 117 homegrown terrorist cases and is a product of over a year and half of extensive research on homegrown terrorism. The study shows that there is no single path to radicalization, nor one factor found in all cases. Rather, different individuals are influenced by different factors. The study finds that the demographics of homegrown terrorists in the United States and United Kingdom do not align with existing jihadist profiles: married, educated, and middle class. Rather, the homegrown terrorists examined were generally unmarried, less educated, and came from a lower socioeconomic background.

Similarly, the study challenges the prevailing thought that religion plays a minimal role in the radicalization process and that political factors are most significant. While political grievances are important, five of the six manifestations identified in the radicalization process were religious. The study finds that many of the individuals studied tended to seek guidance from a select group of religious authorities, many of whom ushered the individuals towards the crucial point of taking violent action. The Report went on to discuss countermeasures to homegrown terrorism:

- local policing aimed at lessening the tension between Muslims and law enforcement agencies;
- improving the understanding of law enforcement of the stages of radicalization;
- Muslim civic engagement, through which local religious leaders can combat domestic radicalism by reaching out to disaffected, young individuals in their communities;

It noted that any comprehensive law enforcement model should consider prevention-oriented, intelligence-led policing techniques. In the United Kingdom, counter-radicalization programs aim to understand how religion can shape communities positively. For example, Quilliam Foundation, a London think tank, works with British law enforcement officials, as well as Muslim parents, teachers, and community leaders, to debunk radical propaganda.[70]

---

68 Page 16 of the Report.

69 Available at http://www.defenddemocracy.org/downloads/HomegrownTerrorists_USandUK.pdf.

70 Founders of the Quilliam Foundation are former leading ideologues of U.K.-based extremist Islamist organizations (its website is available at http://www.quilliamfoundation.org/).

In **March 2010**, the Center for Strategic and International Studies released a Report entitled: *A Growing Terrorist Threat? Assessing "Homegrown" Extremism in the United States*.[71] The Report analysed five events of homegrown terrorism in the United States that occurred during the fall of 2009. It stated that policymakers and officials at the national level "must consider new ways to interdict the growing trend of 'Internet radicalization.'"[72] Many of the 2009 fall suspects were connected with transnational terrorist recruiters via the Internet.

---

71 Available at http://csis.org/files/publication/100304_Nelson_GrowingTerroristThreat_Web.pdf.

72 Ibid., p. VI.

CANADA

PREPARED FOR THE SPECIAL SENATE COMMITTEE ON ANTI-TERRORISM

RECENT DEVELOPMENTS IN ANTI-TERRORISM LAW AND POLICY IN AUSTRALIA

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

5 August 2010

INTRODUCTION

This paper provides an overview of some of the recent developments in anti-terrorism law and policy in Australia. It outlines the legislative framework that Australia has put into place to combat and prevent terrorism, and highlights some of the recent case law developments regarding the terrorism provisions contained in various statutes. The paper also provides an update on some of the recent policy initiatives Australia has put into place to deter homegrown terrorism.

LEGISLATIVE FRAMEWORK AND RELEVANT CASE LAW

Since 11 September 2001, Australia has enacted close to 40 pieces of anti-terrorism legislation, mostly influenced by the United Nations Security Resolution 1373[1] and British anti-terrorism laws. Key pieces of Australia's anti-terrorism legislation include:

- The *Security Legislation Amendment (Terrorism) Act 2002*, which created new terrorism offences and other offences relating to terrorist organizations membership. Both Canada and Australia distinguish terrorist crimes from ordinary crimes on the basis that acts of terrorism are designed to advance a political, religious or ideological cause. In *R.* v. *Mallah*,[2] acquittals of terrorism offences were rendered by the Supreme Court of New South Wales on the basis of a failure to prove political or religious motive. However, two Australian Parliamentary Committees have recommended the retention of the motive requirement for these offences.[3]

- The *Telecommunications Interception Legislation Amendment Act 2002*, which permits law enforcement agencies to seek telecommunications interception warrants in connection with the investigation of terrorism offences.

- The *Suppression of the Financing of Terrorism Act 2002*, which created an offence that targets persons who provide or collect funds and are reckless as to whether those funds will be used to facilitate a terrorist act.

- The *Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002*, which made it an offence to place bombs or other lethal devices in prescribed places with the intention of causing death or serious harm or causing extensive destruction which would cause major economic loss.

- The *Criminal Code Amendment (Offences Against Australians) Act 2002*, which amended the *Criminal Code* by inserting new provisions to make it an offence to

---

1 SC Res 1373, UN SCOR, 56th sess., 4385th mtg, UN DOC S/Res/1373 (2001).

2 [2005] NSWSC 317.

3 Security Legislation Review Committee, *Report of the Security Legislation Review Committee* (2006); Parliamentary Joint Committee on Intelligence and Security, *Review of Security and Counter-Terrorism Legislation* (2006), Recommendation 7. In Canada, the Special Senate Committee on Anti-Terrorism recommended removing the motive requirement as it may encourage racial and religious profiling during investigations (Report of the Special Senate Committee on Anti-Terrorism, *Fundamental Justice in Extraordinary Times* (2007), Recommendation 1).

murder, commit manslaughter or intentionally or recklessly cause serious harm to an Australian outside Australia.

- The *Australian Security Intelligence Organization Legislation Amendment (Terrorism) Act 2003* and the *ASIO Legislation Amendment Act 2003*, which empowers the Australian Security Intelligence Organization (ASIO) to obtain a warrant to detain and question a person who may have information important to the gathering of intelligence in relation to terrorist activities.

- The *National Security Information (Criminal and Civil Proceedings) Act 2004*, which protects information from disclosure in federal criminal proceedings where the disclosure would be likely to prejudice Australia's national security. Like section 38 of the *Canada Evidence Act*, it requires participants to notify the Attorney General in advance with respect to the disclosure of information that may be injurious to national security. Even though the Australian Act appears to give greater weight to risks to national security than its Canadian counterpart, the Supreme Court of New South Wales upheld the constitutionality of the legislation in 2006.[4]

- The *Anti-Terrorism Act (No. 2) 2004*, which created an offence to intentionally associate with a person who is a member of a listed terrorist organization.

In December 2005, in response to the London bombings of July 2005 and to the arrests of suspected terrorists in Sydney and Melbourne in November 2005, Australia enacted the *Anti-Terrorism Act (No. 2) 2005* to authorize preventive detention and control orders for terrorist suspects. The Australian provisions, provide for the preventive detention of a person for up to 72 hours without charge where it is reasonably necessary to prevent a terrorist activity.[5] The consent of the Attorney General is not required and the detention period can be extended by state legislation.[6] Control orders provide for the monitoring of terrorist suspects who pose a risk to the community.[7] They can be granted on the basis that they would assist in preventing a terrorist act or when a person has trained with a terrorist organization.

Unlike preventive detention orders, control orders can only be made with the Attorney General's consent and only be issued by a judge for a period of 12 months. The legislation specifically lists possible conditions that may accompany such orders, including wearing a tracking device, prohibition from using specific forms of telecommunication technologies (including the Internet), and not associating with specific individuals. In 2007, the Australian High Court upheld the constitutional validity of control orders made under terrorism legislation.[8]

The *Anti-Terrorism Act (No. 2) 2005* also dealt with speech associated with terrorism. It allowed organizations to be proscribed on the basis that they advocate the commission of a

---

4 *R.* v. *Lodhi*, [2006] NSWSC 571.

5 *Criminal Code Act 1995*, Division 105.

6 For example, prevention detention orders under New South Wales legislation allow detention for up to 14 days (*Terrorism (Police Powers) Act 2002* (NSW) s.26k).

7 *Criminal Code Act 1995*, Division 104.

8 *Thomas* v. *Mowbray [2007] HCA 33* (2 August 2007).

terrorist act.[9] It also revised Australian sedition offences to include speech that intentionally urges, through the Internet or other means of communication, persons to assist organizations or countries that are engaged in hostilities against the Australian Defence Forces or engaged in a declared or undeclared war against Australia.[10] In 2009, Belal Khazaal was found guilty by the Supreme Court of New South Wales of inciting terrorism by producing a book on how to wage a jihad and sentenced to 12 years' imprisonment.[11]

In 2006, the *ASIO Legislation Amendment Act 2006* amended the *Australian Security Intelligence Organization Legislation (ASIO) Legislation*, which allowed the detention for compelled questioning of persons with information about possible terrorist offences. The detention could be ordered for renewable 48-hour periods and without access to legal advice. The *ASIO Legislation Amendment Act 2006* provided the person questioned or detained under ASIO warrants with the right to consult a lawyer. The *ASIO Legislation Amendment Act 2006* also extended the ASIO provisions, which were subject to a sunset clause, until 2016.[12]

In September 2007, the *Communications Legislation Amendment (Crime or Terrorism Related Internet Content) Bill 2007* was introduced in the Australian Senate, however it died with the 2007 November elections before becoming law. The bill would have expanded the "black list" of Internet addresses that is currently maintained by the Australian Communications and Media Authority (ACMA) to include terrorism and cybercrime sites. It would have allowed the Australian Federal Police to notify the ACMA in writing of websites that they had reason to believe were crime or terrorism-related. In response to such notice, the ACMA would have been required to notify Internet service providers (ISPs) of the crime or terrorism-related content. ISPs notified by the ACMA would then have been required to take reasonable steps[13] to prevent end-users of their Internet service from accessing that crime or terrorism-related Internet content.

In June 2009, the *Independent National Security Legislation Monitor Bill 2010* was introduced in the Australian Senate and became law in April 2010. It established the position of the National Security Legislation Monitor, whose functions will be to review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation and report his or her comments, findings and recommendations to the Prime Minster and Parliament, on an annual basis. As well, the Monitor is required to consider whether Australia's counter-terrorism and national security legislation contains appropriate safeguards for protecting individuals' rights and continues to be necessary. The

---

9 *Criminal Code Act 1995*, s. 102.1

10 *Criminal Code Act 1995*, s. 80.2.

11 *R.* v. *Khazaal*, [2009] NSWSC 1015 (25 September 2009).

12 Most of the information provided in the above paragraphs comes from: Kent Roach, "A Comparison of Australian and Canadian Anti-Terrorism Laws," HeinOnline, 30 U.N.S.W.L.J. 53, 2007.

13 Such as blocking sites using filters.

main purpose of the legislation is to ensure the laws operate in an effective and accountable manner, are consistent with international human rights law and help to maintain public confidence in those laws.

In March 2010, the *National Security Legislation Amendment Bill 2010* was introduced in the House of Representatives and was at second reading in the Senate in June 2010. This Bill implements a package of reforms to Australia's national security legislation, announced by the Australian government in August 2009. Many of the proposed provisions in the bill will implement the government's response to several independent and bipartisan parliamentary committee reviews of Australian national security and counter-terrorism legislation. Some of the proposed amendments include:

- Amending the definition of "advocates" to clarify that an organization advocates the doing of a terrorist act if the organization directly praises the doing of a terrorist act in circumstances where there is a *substantial risk* that such praise might have the effect of leading a person to engage in a terrorist act.

- Extending the period of a regulation that lists a terrorist organization from two to three years.

- Improving the standard for listing a person or entity in order to implement the Australian government's response to recommendation 22 of the Parliamentary Joint Committee on Intelligence and Security's Report Review of Security and Counter-Terrorism Legislation, tabled in Parliament in December 2006.

POLICY INITIATIVES

Australian security authorities have identified that Australians are at risk of being terrorist targets both at home and abroad, including from homegrown extremists, and that this risk will continue for some time. As an example of the homegrown terrorism threat in Australia, it could be noted that of the 38 offenders prosecuted for terrorism in Australia, 37 were Australian citizens, and 20 were born in Australia.[14]

In 2005–2006, the Australian Ministerial Council on Immigration and Multicultural Affairs developed a National Action Plan, at the request of the Council of Australian Governments.[15] It responded to the particular pressures Australian communities were facing as a result of increased intolerance and the promotion of violence arising from events around the world and in Australia since 2001. It addressed issues of marginalization, promoted understanding and dialogue among all Australians and built on existing government programs, focusing on four key areas: education, employment, integration and security. This coordinated government and community long-term approach

---

14 Joint press conference on the Counter-Terrorism White Paper, February 2010, http://www.foreignminister.gov.au/transcripts/2010/100223_jpc_pm.html.

15 Ministerial Council on Immigration and Multicultural Affairs, *A National Action Plan to Build on Social Cohesion, Harmony and Security*, http://www.immi.gov.au/living-in-australia/a-diverse-australia/national-action-plan/_attach/National-Action-Plan-2007.pdf.

calls for further research to be undertaken into the causes of extremism, the potential for the radicalization process to result in violence and disruption, and the extent to which extremism is present in Australia. Some of the main goals of the National Action Plan are:

- Reducing the vulnerability of Australians to extremist recruiters through targeted education, mentoring and employment programmes and initiatives;
- Supporting educational and community programs and projects encouraging loyalty and commitment by all Australians to their country, especially its parliamentary democracy and legal structures, and the promotion of Australian values;
- Building leadership capacity in communities, members of which might be susceptible to radicalization, so that all leaders can be proactive in addressing the potential for extremism within their own communities;
- Promoting and building closer collaboration, liaison, information-sharing and trust between governments and communities and encouraging increased participation in mainstream Australia by those communities currently feeling disengaged or marginalized.

In February 2010, the Australian government released the Counter-Terrorism White Paper.[16] It underlined the changing nature of the terrorist threat to Australia and the continuing rise of homegrown terrorists. In the chapter on resilience, the White Paper explains, in general terms, how Australia intends to counter violent extremism.[17] It states that the Australian government must work with communities to:

> provide information on [the government] counter-terrorism efforts and basic facts about domestic initiatives and foreign policy; seek to address grievances that could encourage a receptiveness to violent extremism; and provide opportunities for people at risk of violent extremism to actively participate in Australia's economy, society and democratic processes.[18]

However, the White Paper does not offer any new programs or funding to counter homegrown extremist ideology comparable to, for example, the British counter-terrorism strategy, Contest Two, that committed £100 million towards preventing individuals from becoming terrorists.

---

16 See http://www.dpmc.gov.au/publications/counter_terrorism/docs/counter-terrorism_white_paper.pdf.

17 Counter-Terrorism White Paper, Chapter 7, pp. 65–68.

18 Ibid., p. 67.

CANADA

PREPARED FOR THE SPECIAL SENATE COMMITTEE ON THE ANTI-TERRORISM

RECENT DEVELOPMENTS IN ANTI-TERRORISM LAW AND POLICY IN FRANCE

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

5 August 2010

INTRODUCTION

This paper provides an overview of some of the recent developments in anti-terrorism law and policy in France. It outlines the legislative framework that France has put into place to combat and prevent terrorism, and highlights some of the recent case law developments regarding the terrorism provisions contained in various statutes. The paper also provides an update on some of the recent policy initiatives France has put into place to deter homegrown terrorism.

LEGISLATION FRAMEWORK AND RELEVANT CASE LAW

The legislation in France applicable to the fight against terrorism dates from the mid-1980s, and was developed over France's recent decades of experience with transnational and domestic-origin terrorism. Accordingly, when combating Islamist terrorism became an international priority, following on the attacks committed in the United States on 11 September 2001, France already had a sophisticated anti-terrorism framework in place.

In response to the threat presented by domestic and international terrorism, France has adopted a preventive approach that focuses on three main priorities: information gathered by intelligence services; aggressive prosecutions with the intention of dismantling nascent terrorist networks; and deportation of foreign nationals suspected of terrorist activities or accused of fomenting radicalization and recruiting for terrorist purposes.

In 1986, France enacted its fundamental anti-terrorism legislation: Loi n° 86-1020 of 9 September 1986. This legislation established a centralized judicial system for dealing with offences associated with terrorism, and created a specialized body of examining magistrates [*juges d'instruction*] and prosecutors based in Paris – the Service central de lutte antiterroriste, commonly referred to as the 14th section of the prosecutor's office – to handle all terrorism cases. The 1986 law also instituted trials for terrorism offences before professional magistrates in the Cour d'assises de Paris, as an exception to the rule that trials in the *cour d'assises* are held before a lay jury. The Conseil constitutionnel concluded that replacing lay juries with professional judges in terrorism-related cases was an appropriate way of avoiding pressure and threats to jury members.[1]

The 1986 law also lengthened the period of time during which an accused may be held in custody before being arraigned [*garde à vue*], increasing it to 96 hours (four days) from 48, in terrorism-related cases.[2] In response to the bombings in London on 7 July 2005, Loi n° 2006-64 of 23 January 2006 further extended the maximum time to 144 hours (six days) in cases where there is a serious risk of an imminent terrorist attack or if the

---

1 Décision n° 86-213 DC. The Conseil constitutionnel is composed of nine judges who decide the constitutionality of legislation, among other things. In Canada, section 11(f) of the *Canadian Charter of Rights and Freedoms* guarantees an accused the right to a trial by jury where the maximum punishment for the offence is imprisonment for five years or a more severe punishment.

2 In ordinary criminal cases in France, the police may arrest suspects and hold them in pre-arraignment custody for a maximum of 24 hours, with the possibility of extending custody for 24 hours, after which they must release them or take them before an examining magistrate for their appearance.

complexity of the case and the need for international cooperation makes it necessary.[3] In Canada, the 2001 *Anti-terrorism Act* allowed for preventive detention for a maximum of 72 hours (three days) before the person concerned was required to appear before a judge.[4] As well, persons suspected of terrorism held in pre-arraignment custody in France have very limited access to counsel. They do not have access to the services of a lawyer until after the first 72 hours or, in certain circumstances, 96 hours. And although a special parliamentary inquiry into the Outreau case[5] recommended that police questioning conducted during pre-arraignment custody be recorded for all offences,[6] one of the effects of Loi n° 2007-291 of 5 March 2007, which came into force in June 2008, was to preclude audiovisual recordings in the case of terrorism-related offences.

The most important aspect of French anti-terrorism legislation is the offence of criminal association in relation toa terrorist enterprise. That offence was introduced by Loi n° 96-647 of 22 July 1996, which authorizes officials to take preventive measures prior to the commission of a terrorist act. The offence in question is broadly defined as the act of [Translation] "participating in a group formed, or an agreement made, for the purpose of preparing for the commission of one or more acts of terrorism as set out in the preceding sections, by the commission of one or more concrete acts."[7] Acts of terrorism include offences such as intentional endangerment of life, intentional endangerment of safety, firearms offences, money laundering and certain property offences committed for the purpose of causing serious interference with the public interest by intimidation or terror.[8]

The elements of the offence of criminal association that have been developed by the French courts include the following: there must be a group of persons who come together with the intent of committing a joint criminal act; each member of the group must have full knowledge of that intent and of the fact that group is a criminal enterprise; and one or more concrete acts must have been committed to demonstrate that intent. If these three conditions are met, a court may find an individual guilty of criminal association in relation to that a terrorist act has been perpetrated by an individual, despite the fact that the individual in question may not have committed a concrete terrorist activity him or herself.[9]

---

3 *Code de procédure pénale*, arts. 706-88.

4 Former s. 83.3 of the *Criminal Code*. That section and ss. 83.28 and 83.29 concerning investigative hearings were subject to a sunset clause. They were not renewed and so have ceased to apply. Current Bill C-17 provides for them to be reintroduced into Canadian law. Until Bill C-17 is passed, the 24-hour time limit provided in the ordinary law applies (or, if a justice is not available within that time, as soon as possible after arrest: s. 503 of the *Criminal Code*). As well, s. 810.01 of the *Criminal Code* of Canada still provides that a judge may impose a recognizance to keep the peace if a person fears on reasonable grounds that another person will commit a terrorism offence.

5 The Outreau case involved crimes of sexual assaults against children and culminated in a notorious judicial error in France.

6 Assemblée Nationale, Rapport n° 3125, 6 June 2006.

7 *Code pénal*, art. 421-2-1.

8 *Code pénal*, art. 421-1 (as amended by Loi n°2005-1550 of 12 December 2005).

9 The fact that the criminal association offence need not be connected with any terrorist act has generated criticism (see International Federation for Human Rights, "France: paving the way for arbitrary justice," No. 271-2, 1999).

In most cases, the offence of criminal association in relation to a terrorist enterprise is considered to be an offence punishable by a maximum term of imprisonment for 10 years.[10] Loi n° 2006-64, which was enacted in response to the London bombings, increased the penalty associated with this offence to a maximum term of imprisonment for 20 years where the criminal association was formed for the purpose of preparing for one of the following acts: endangering life or safety; kidnapping; forcible confinement; interference with any mode of transportation; destruction by means of explosive or incendiary substances in circumstances likely to result in death; introducing a substance capable of endangering health into the atmosphere, the soil, the subsoil, food or food ingredients, or water. Loi n° 2006-64 also increased the sentence applicable for a person found to be in charge of a criminal organization to 30 years from 20 years. In addition, sentences for all criminal offences may be increased where they are committed in connection with a terrorist intent. For example, endangering life, for which a maximum term of imprisonment of 30 years may be imposed, may be subject to imprisonment for life if it is committed in connection with a terrorist act.[11]

As well, Loi n° 2006-64 enabled France to create a national list of persons and entities involved in acts of terrorism. The 2006 law and three other major pieces of legislation enacted between 2001 and 2004[12] also extended police powers to conduct inspections of vehicles and buildings, imposed an obligation on Internet and telecommunications service providers to retain and disclose data, required that encryption codes be disclosed when disclosure is determined to be necessary in a terrorism investigation, strengthened security measures in airports and ports, enhanced surveillance measures in general and instituted new measures to combat the financing of terrorism.

Loi n° 2007-1443 of 9 October 2007 established a parliamentary oversight mechanism for French intelligence services. The law created a special parliamentary delegation composed of four members of parliament and four senators. The delegation holds all its hearings *in camera* and its proceedings are subject to national defence privilege. It may also make recommendations to the Prime Minister and the President. The delegation officially commenced its work in February 2008.[13]

---

10 In Canada, for example, the offence participation in an activity of a terrorist group is subject to similar punishment: imprisonment for a term not exceeding 10 years (s. 83.18 of the *Criminal Code*). It is worth noting that like the French law, paragraph 83.18(2)(*a*) of the *Criminal Code* of Canada does not require that a terrorist activity have actually been committed or facilitated in order for a person to be convicted of the offence of participation in an activity of a terrorist group.

11 *Code pénal*, art. 421-3.

12 Loi n° 2001-1062 of 15 November 2001 relating to the safety of everyday life, Loi n° 2003-239 of 18 March 2003 relating to domestic security, and Loi n° 2004-204 of 9 March 2004 adapting the justice system to the changing nature of crime.

13 The United Kingdom and the United States, for example, also have a parliamentary oversight mechanism for their intelligence services. In Canada, in October 2004, the Interim Committee of Parliamentarians on National Security recommended the creation of a Parliamentary Intelligence Committee with responsibility for ensuring that the security and intelligence community is effectively serving Canadian interests, is respecting the *Canadian Charter of Rights and Freedoms* and is fiscally responsible and properly organized and managed. In November 2005, Bill C-81 proposed that a parliamentary committee responsible for national security be created, but the bill died on the Order Paper when the 38th Parliament was dissolved. In 2007, the Special Senate Committee on the *Anti-terrorism Act* recommended in its report *Fundamental Justice in Extraordinary Times* that "a standing committee of the Senate, with dedicated staff and resources, be established to monitor, examine and periodically report on matters relating to Canada's anti-terrorism legislation and national security framework on an ongoing basis" (recommendation 39).

POLICY INITIATIVES

France has stressed the need to supplement enforcement action with preventive political action. The French government presented its vision in March 2006 in its white paper on domestic security in the face of terrorism.[14] The white paper notes a shift in the scope, distribution, operating methods and effectiveness of terrorist networks since the bombings in Madrid in 2004 and in London in 2005,[15] and stresses that the primary aggravating factor is the development of a generation of [TRANSLATION] "homegrown rebels," whether French citizens or otherwise, and whether Muslim of long standing or recent converts.[16]

One of the proposals in the white paper to combat that threat posed by domestic terrorism is an inclusive government communications strategy to rally the public around common human values, with the aim of precluding extremist and violent speech and isolating terrorists. The communications strategy focuses on two priorities:

> The first consists of recognizing and reaffirming that Arab and Muslim countries exist in symbiosis, rather than conflict, with western civilization. The second consists of targeting communications to the middle classes and young generations, including where they see their spaces of expression curbed by their leaders.[17] [Translation]

The preventive strategy is to include organizing national or regional conferences, meetings to be held with the goal of bringing people with special credibility among the populations targeted by terrorists into the conversation, among other things. In 2010, a research project funded by the Government of Canada and carried out by a think tank in the United Kingdom, on the phenomenon of domestic terrorism in the United Kingdom, Canada, Denmark, the Netherlands and France recommended:

> Governments and policing agencies should work with radicals in certain instances where there are specific tactical benefits, for example in local de-radicalisation programmes. In some cases–especially when working with an individual who believes violence is religiously obligated, or may be tempted by these ideas–non-violent radicals can sometimes have the credibility needed to convince them otherwise.[18]

---

14 Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme, *La France face au terrorisme*, 2006, http://lesrapports.ladocumentationfrancaise.fr/BRP/064000275/0000.pdf (accessed on 5 August 2010).

15 See also Livre blanc du Gouvernement sur la défense et la sécurité intérieure, 2008, http://www.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/livre_blanc_1337/livre_blanc_1340/index.html (accessed on 5 August 2010).

16 Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme, *La France face au terrorisme*, 2006, p. 35.

17 Ibid., p. 123.

18 Jamie Bartlett, Jonathan Birdwell and Michael King, *The edge of violence, a radical approach to extremism*, 2010, p. 17, http://www.demos.co.uk/files/Edge_of_Violence_-_web.pdf?1271346195 (accessed on 5 August 2010).

As well, the communications strategy advocated in the French government's white paper rules out a specific policy of communication with terrorists, [Translation] "because a policy of that kind could only offer them reassurance by presenting them as recognized interlocutors. It would merely strengthen their attraction for potential recruits or supporters."[19] It stresses that special attention should be given to the dissemination of racist or anti-Semitic ideas or ideas that provoke terrorism in satellite television broadcasts.

The white paper also cautions against the dangers of developing policy based on prejudice:

> We must avoid falling into the trap of the 'war of civilizations' held up to us by Islamist-inspired international terrorism and reject the conflation of Islam and terrorism into which it would like to lead us. France demonstrates its rejection of that conflation when it encourages the organization of Islam in France, for example through the Conseil français du culte musulman,[20] when it engages in ongoing pressure at the international level for better dialogue between peoples, in particular with our neighbours in the South and the Muslim world, and when it combats all forms of hate speech.[21] [Translation]

It also stresses the importance of mutual openness between societies with Muslim cultures and western societies. The white paper notes that at the Barcelona summit in November 2005, countries in the Euro-Mediterranean partnership found common ground for the first time on the fight against terrorism, by adopting a "code of conduct." They expressed the unanimous opinion that terrorism is unjustifiable and stated their intention to implement the United Nations conventions on combating terrorism.

In 2006, a fund was created to compensate victims of terrorist acts committed in France and French citizens who are victims of terrorist acts abroad and their survivors, regardless of nationality.[22] However, compensation may be denied or reduced if there was fault on the part of the victim.

On 18 January 2010, the French government created the Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme. The primary goal of the Conseil is to ensure better coordination between government agencies and oversight authorities involved in combating money laundering and the financing of terrorism, in order to strengthen the effectiveness of those efforts and monitor the preparation and regular updating of a comprehensive document concerning the threat presented by money laundering and the financing of terrorism.

---

19 Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme, *La France face au terrorisme*, 2006, p. 122.

20 The Conseil français du culte musulman, created in 2006, is involved in activities in respect of relations with the French government and the construction of mosques, for example.

21 Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme, *La France face au terrorisme*, 2006, p. 10.

22 Subsection 83.14(5.1) of the *Criminal Code* of Canada authorizes the use of any proceeds that arise from the disposal of property forfeited in relation to a terrorist activity to compensate victims of terrorist activities and to fund anti-terrorist initiatives.