PRB 05-83E

Library of Parliament Bibliothèque du Parlement

THE USA PATRIOT ACT AND CANADA'S *ANTI-TERRORISM ACT*: KEY DIFFERENCES IN LEGISLATIVE APPROACH

Jennifer Wispinski
Law and Government Division

31 March 2006

PARLIAMENTARY INFORMATION AND RESEARCH SERVICE
SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES

TABLE OF CONTENTS

Page

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

THE USA PATRIOT ACT AND CANADA'S *ANTI-TERRORISM ACT*: KEY DIFFERENCES IN LEGISLATIVE APPROACH

INTRODUCTION

Following the 11 September 2001 terrorist attacks in the United States, the U.S. Congress passed 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).(1) Canada also enacted a legislative response to the events of 11 September 2001: the *Anti-terrorism Act*.(2) Both statutes were speedily enacted, intended to address the threat posed by the attacks and designed to give government agencies additional tools and powers to prevent and combat terrorism. However, there are key differences between the Canadian and American legislative approaches, some of which arise as a result of differences between the pre-existing legislative frameworks of the two countries, and some of which appear to arise from decisions, on the part of legislators, to approach similar problems differently.

This paper provides an overview of several differences in legislative approach taken under the Patriot Act and the *Anti-terrorism Act*. It focuses on six key areas:

- new crimes and penalties;
- new investigative tools and procedures;
- electronic surveillance and communications interception;
- information gathering, secrecy and sharing;
- the listing of terrorist entities; and
- the suppression of terrorist financing.

---

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

(2) S.C. 2001, c. 41.

This paper also discusses the sunset and/or review provisions contained in both Acts and provides information on the two statutes that have amended the Patriot Act: the USA PATRIOT Improvement and Reauthorization Act of 2005 and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006.

NEW CRIMES AND PENALTIES

Prior to the coming into force of the *Anti-terrorism Act*, Canada's *Criminal Code*[3] did not contain a definition of "terrorist activity." The *Anti-terrorism Act* introduced broad definitions of both "terrorist activity" and "terrorist group" into the Code. "Terrorist activity" is defined in section 83.01(1) to include any act or omission committed inside or outside of Canada that, if committed in Canada, is one of the terrorist offences referred to in ten anti-terrorist international conventions into which Canada has entered. It is also defined to include a variety of other acts or omissions committed inside or outside of Canada, either partially or wholly, for political, religious or ideological purposes, causes or objectives.[4] Although broad in scope, or perhaps because of its breadth, the definition of terrorist activity includes certain saving provisions designed to ensure that activities related to lawful armed conflict under international law, advocacy, protest, dissent or work stoppage, or the mere expression of a political, ideological or religious belief, without more, will not be considered "terrorist activity."

The definition of "terrorist group" as set out in section 83.01(1) of the Code is similarly broad. While the definition of "terrorist group" appears narrower and simpler on its face, it incorporates the definition of "terrorist activity" by reference, thus incorporating that definition's breadth and complexity.

The *Anti-terrorism Act* also introduced several new terrorism offences into the Code. Because the new offences incorporate the definitions of "terrorist activity" and "terrorist group" by reference (for example, participation in the activities of a terrorist group under section 83.18, or facilitating a terrorist activity under section 83.19), the new offences have an ambit as extensive as the definitions they incorporate. The new offences created under the Code were, however, specifically designed to capture the activities of terrorists or terrorist groups.

---

(3) R.S.C. 1985, c. C-46.

(4) There are no political, religious or ideological motive requirements in the U.S. definitions of terrorism.

The situation under U.S. law is quite different. Whereas no definition of "terrorist activity" existed in Canada's *Criminal Code* before the *Anti-terrorism Act* came into force, the United States Code (U.S.C.)[5] contained both a definition of "international terrorism"[6] 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,[7] 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."[8] Like the *Anti-terrorism Act* in relation to Canada, the Patriot Act also 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 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.

---

(5) The United States Code (Federal Alcove; Reserve) or U.S.C. is the codification by subject matter of the general and permanent federal laws of the United States. It 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.

(6) 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.

(7) 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.

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

NEW INVESTIGATIVE TOOLS AND PROCEDURES

The *Anti-terrorism Act* introduced provisions into the *Criminal Code* that served to provide law enforcement officials with two new investigative tools: investigative hearings and preventive arrests.

Section 83.28 of the *Criminal Code* governs investigative hearings. Such hearings are available only in the case of terrorist offences that have been committed or that may be committed. Section 83.28 allows a peace officer, upon obtaining prior consent of the Attorney General, to apply to a superior or provincial court judge for an order allowing him/her to gather evidence with respect to a terrorist offence. The judge may make this order only if he/she is satisfied that there are reasonable grounds to believe that a terrorism offence has been or will be committed, and that the individual specified in the request for the order may have information concerning the offence. If the judge grants the order, the individual named in it may be compelled to attend a hearing before a judge, answer questions, and bring along anything in his/her possession. A person required to attend an investigative hearing is entitled to retain and instruct counsel. While that person must generally answer the questions posed to him/her, he/she may object to doing so on the basis of law related to disclosure or privilege, and the judge will decide whether or not to uphold the objection. Finally, while a person required to attend the investigative hearing cannot refuse to answer questions or produce things on the grounds that the answers or things might incriminate him or her, information or testimony obtained from a person during such a hearing cannot be used against him or her in subsequent proceedings, except in a prosecution for perjury.

Section 83.3 of the *Criminal Code* governs preventive arrests. Under this section, a peace officer who believes on reasonable grounds that a terrorist activity will be carried out and suspects on reasonable grounds that imposing a recognizance with conditions on, or the arrest of, a person is necessary to prevent the carrying out of this activity, may, after obtaining the prior consent of the Attorney General, lay an information concerning that person before a provincial court judge, who may, in turn, on the basis of that information, order that person to appear before him or her. Once an information has been laid and a summons issued or, alternatively, if there are grounds for laying the information and it cannot be laid due to exigent circumstances, a peace officer may arrest the person without warrant and detain that person in custody if he or she suspects on reasonable grounds that detention is necessary in order to prevent a terrorist activity.

A person detained after such an arrest must be brought before a provincial court judge within 24 hours, or as soon as possible thereafter. At that time, a hearing must be held in order to determine whether the person's continued detention is warranted. This "show cause" hearing can be adjourned, if necessary, but only for up to 48 hours. After the hearing, if the judge determines that there is no need for the detained person to enter into a recognizance, then he or she is released. If the judge determines that the person should enter into a recognizance, the judge may impose terms and conditions on his or her release, requiring him or her to, for example, keep the peace or to not be in possession of a weapon. The length of the recognizance cannot exceed 12 months. If the person in question refuses to enter into a recognizance, the judge can order that he or she be jailed for up to 12 months.

With respect to the situation in the United States, there was no need to introduce investigative tools comparable to investigative hearings or preventive arrests through the Patriot Act because U.S. law already contained roughly equivalent tools: the grand jury process and the material witness arrest process. Having said this, the Patriot Act did introduce 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.[9] 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. Unlike the situation in Canada, where a person cannot refuse to answer questions during an investigative hearing on the basis that the answer may be self-incriminating, under the U.S. grand jury system, the privilege against self-incrimination applies. However, where a witness asserts the self-incrimination privilege, the grand jury can often get at the information another way, by subpoenaing a third-party witness to

(9) 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.).

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, and, if necessary, interpreters.(10) 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).(11) 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(12) or foreign intelligence to be released to a wide variety of federal officials to assist them in the performance of their duties.(13) Although section 203(a) introduces a notification safeguard, requiring courts to be confidentially notified when disclosure has been granted to such federal officials,(14) 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 could be easily abused by government officials.

With respect to the material witness arrest process, it, like the grand jury process, predates the enactment of the Patriot Act.(15) The federal government in the United States may

---

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

(11) F.R.Crim.P. 6(e). For a through 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.

(12) Under the Patriot Act, foreign intelligence and counterintelligence are broadly defined terms.

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

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

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

use this process to arrest a witness in order to secure his or her testimony in a criminal proceeding.(16) 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.(17) Because it can be used to investigate any offence, not just terrorist offences, the material witness arrest process in the United States has a wider application than Canada's preventive arrest process.

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.(18) There is a judicial presumption in favour of release, unless there is probable cause to believe the person has committed certain types of serious federal offences, one of which is the federal crime of terrorism.(19) If the person is released, the judge may impose conditions on the release.(20) Unlike the situation in Canada with respect to preventive arrest, 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 is being used, it was used after 9/11 to detain approximately 70 individuals, primarily Muslim men, so as to facilitate the investigation of terrorist crimes. The American Civil Liberties Union (ACLU) and Human Rights Watch have stated 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.(21)

---

(16) Under U.S. law, a criminal proceeding includes a grand jury proceeding.

(17) 18 U.S.C. 3144.

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

(19) 18 U.S.C. 3142(a), (b) (e) and (f).

(20) 18 U.S.C. 3142(c).

(21) 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 Web site 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 on-line by Human Rights Watch and the ACLU on 27 June 2005 and available at: http://hrw.org/reports/2005/us0605.

ELECTRONIC SURVEILLANCE AND COMMUNICATIONS INTERCEPTION

The Canadian legislative approach to electronic surveillance and communications interception was not altered significantly by the *Anti-terrorism Act*. In almost all cases, prior judicial authorization is still required before electronic surveillance or communications interception can be conducted by Canadian authorities.(22) The sole exception to this is when "private communication"(23) is intercepted by the Communications Security Establishment (CSE),(24) in which case prior authorization from the Minister of National Defence is required.(25) There are many safeguards contained in the provisions authorizing CSE interceptions that are designed to limit when such interceptions can be authorized and how the intercepted information may be used once captured (for example, the interception must be directed at foreign entities outside of Canada, or, in the case of interceptions for the purpose of protecting Government of Canada computer systems or networks, the interception must be necessary to isolate or prevent harm to these systems or networks, it must be demonstrated that the information could not reasonably be obtained through other means, the expected foreign intelligence value of the interception must justify interception, or, in the case of interceptions to protect Government of Canada computer systems or networks, the consent of those whose private communications may be intercepted cannot reasonably be obtained, and, in the event of an interception, satisfactory measures must be in place to protect the privacy of Canadians).(26)

---

(22) This includes communications interceptions conducted for foreign intelligence purposes by the Canadian Security Intelligence Service (CSIS). See sections 21 to 28 of the *Canadian Security Intelligence Service (CSIS) Act*, R.S.C. 1985, c. C-23.

(23) Under section 273.61(1) of the *National Defence Act*, R.S.C. 1985, c. N-5, which was added to that Act by section 102 of the *Anti-terrorism Act*, "private communication" has the same meaning as in section 183 of the *Criminal Code*. Section 183 of the *Criminal Code* defines "private communication" as "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it."

(24) The CSE is Canada's signals intelligence interception agency. It was established after World War II and transferred to the Department of National Defence in 1975. It was given a statutory or legislative existence and mandate for the first time under the *Anti-terrorism Act.* Section 102 of the Act added sections 273.61 to 273.7 to the *National Defence Act.* These sections provide the CSE with its mandate and powers.

(25) See sections 273.65(1) and (3) of the *National Defence Act*.

(26) See sections 273.65(2), (4) and (5) of the *National Defence Act*.

By contrast, U.S. legislation had tiers of privacy protection when it came to electronic surveillance even before the Patriot Act was enacted. 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).

The Patriot Act has 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)[(27)] 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 allowing 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.[(28)]

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.[(29)] 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).

---

(27) See 50 U.S.C., Chapter 36, which contains FISA.

(28) 50 U.S.C. 1805(c)(2)(D) and 1805(d).

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

It would appear that the United States has also done away with the need for prior judicial authorization for electronic surveillance in certain circumstances. On 16 December 2005, *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 e-mails 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.(30) Following the release of this article, the President confirmed that he had, in fact, signed such an order.(31) He and his advisors have 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(32) 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,(33) which was signed into law by President Bush on 18 September 2001.(34) The AUMF resolution authorized the President to use "all necessary and appropriate force against those nations, organizations, or persons he determines planned, 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.(35)

---

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

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

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

(33) See the White House, Press Release, "Press Conference of the President," 19 December 2005, available on-line at: http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html; the White House, Press Release, "Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence," 19 December 2005, available on-line at: http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html; and Assistant Attorney General William Moschella, Letter to the leaders of the Senate and House of Representatives Intelligence Committees, 22 December 2005, available on-line at: http://www.nationalreview.com/pdf/12%2022%2005%20NSA%20letter.pdf.

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

(35) 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' Web site at: http://www.fas.org/sgp/crs/natsec/RS22357.pdf.

Various persons and organizations have, however, expressed concern that the President may not have had the necessary constitutional and/or congressional authority to issue his 2002 Executive Order. They have 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.(36) In addition, some have questioned 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.(37) These concerns and questions have prompted certain civil liberties organizations to take action. On 17 January 2006, two separate lawsuits were filed challenging the legality of the NSA warrantless surveillance program, one filed by a coalition of civil liberties organizations led by the ACLU against the NSA,(38) and the other filed by the Center for Constitutional Rights (CCR) and some of its lawyers and staff against President Bush, the NSA and the Federal Bureau of Investigation, among others.(39) The ACLU-led coalition alleges that the NSA program violates the 1st (freedom of speech) and 4th Amendments of the U.S. Constitution, as well as the constitutional separation of powers principles governing the President and Congress. The coalition seeks a declaration that the program is unconstitutional and an injunction preventing the NSA from continuing the program.(40) The CCR lawsuit alleges that information subject to attorney-client privilege has

---

(36) See, for example, the comprehensive legal analysis of these matters contained in Elizabeth Bazan and Jennifer Elsea, Memorandum, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, Congressional Research Service, Washington, D.C., 5 January 2006, available on the Federation of American Scientists' Web site 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 Web site at: http://www.americanprogress.org/atf/cf/{E9245FE4-9A2B-43C7-A521-5D6FF2E06E03}/nsa_surveillance.pdf.

(37) While government agencies are generally required to obtain prior authorization from the FISA court before engaging in warrantless surveillance, FISA contains 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).

(38) This lawsuit was filed in the Federal District Court in Detroit.

(39) This lawsuit was filed in the Federal District Court in Manhattan.

(40) See ACLU, Press Release, "ACLU Sues to Stop Illegal Spying on Americans, Saying President Is Not Above the Law," 17 January 2006, available on its Web site at: http://www.aclu.org/safefree/nsaspying/23486prs20060117.html. A copy of the statement of claim filed by the ACLU-led coalition is also available on-line at: http://www.aclu.org/images/nsaspying/asset_upload_file137_23491.pdf.

been intercepted under the NSA warrantless surveillance program, makes the same allegations with respect to constitutional violations made in the ACLU-led lawsuit, and, like the ACLU-led coalition, seeks a declaration of unconstitutionality and an injunction preventing the program from being continued.(41)

When information about the NSA's warrantless surveillance program and the Executive Order authorizing it came to light, various congressional committees indicated their interest in investigating both the program and whether or not the President had the necessary authority, pursuant to the U.S. Constitution and/or the AUMF resolution, to authorize the NSA to conduct warrantless surveillance without legislation amending FISA. On 15 January 2006, for example, the Chairman of the U.S. Senate Committee of the Judiciary (the Senate Judiciary Committee), Arlen Specter, stated that the Senate Judiciary Committee would be holding hearings respecting these matters. Senator Specter refrained, however, from describing the ambit of the Committee's investigation, specifying how many hearings would be held, or indicating whom, apart from the United States Attorney General, Alberto Gonzales, the Committee would ask to testify.(42)

Since Senator Specter's announcement, the Senate Judiciary Committee has indeed been investigating these matters. It appears particularly interested in examining the legality of the program. On 6 February 2006, the Committee heard testimony from Attorney General Alberto Gonzales on this issue.(43) The Committee then held two additional hearings respecting wartime executive power and the NSA's surveillance authority, one on 28 February 2006(44) and another on 28 March 2006.(45)

---

(41) See CCR, Press Release, "CCR Files Suit over NSA Domestic Spying Program," 17 January 2006, available on-line at: http://www.ccr-ny.org/v2/reports/report.asp?ObjID=IahVzRA3n9&Content=693. A copy of the CCR's statement of claim is also available on-line at: http://www.ccr-ny.org/v2/legal/govt_misconduct/docs/NSAcomplaintFINAL11706.pdf.

(42) See D. Jehl, "Specter Vows A Close Look at Spy Program," *The New York Times*, 16 January 2006, p. 11.

(43) During his testimony, Mr. Gonzales reaffirmed the government's position regarding the President's ability to authorize the NSA's warrantless surveillance program, asserting that the President had the necessary authority to do so by virtue of his powers as Commander in Chief under Article II of the U.S. Constitution and the AUMF resolution. A transcript of the U.S. Attorney General's 6 February 2006 testimony before the Senate Judiciary Committee is available on the Committee's Web site at: http://judiciary.senate.gov/testimony.cfm?id=1727&wit_id=3936.

(44) The hearing notice and witness list for the 28 February 2006 hearing is available on the Senate Judiciary Committee's Web site at: http://judiciary.senate.gov/hearing.cfm?id=1770. Unfortunately, a transcript of the witnesses' testimony is not available.

(45) The hearing notice and witness list for the 28 March 2006 hearing is available on the Senate Judiciary Committee's Web site at: http://judiciary.senate.gov/hearing.cfm?id=1825. Unfortunately, a transcript of the witnesses' testimony is not available.

It is possible that the Senate Judiciary Committee will hold additional hearings with respect to the legality of the NSA surveillance program. It is equally possible, however, that it will choose not to do so, particularly if Bill S. 2455, the Terrorist Surveillance Act of 2006, is enacted. Bill S. 2455 was introduced into the Senate on 16 March 2006.(46) If enacted in its current form, this bill would, notwithstanding FISA or any other statute dealing with communications interception, allow the United States Attorney General to authorize electronic surveillance of a target without a court order for up to 45 days in circumstances where: the President determines that the surveillance is necessary to protect the United States, its citizens or its interests; at least one of the parties to the communications is outside the United States; a significant purpose of the surveillance is to obtain foreign intelligence information; and minimization procedures are in place with respect to the surveillance. At the end of that period, the Attorney General would have three choices. He or she could: have the surveillance dropped; seek judicial authorization from the FISA court to continue the surveillance; or certify to two seven-member congressional intelligence subcommittees, one from the Senate and one from the House of Representatives, that the President has determined that continued surveillance of the target is necessary to protect the United States, its citizens and its interests despite the fact that there is insufficient evidence for a warrant, and that continued surveillance is being undertaken in a good faith belief that it will result in the acquisition of foreign intelligence information. Bill S. 2455 also contains clauses creating the two new congressional intelligence subcommittees, giving them an oversight role over the terrorist surveillance program generally and the surveillance of individual targets under the program.

Bill S. 2455 has been referred to the Senate Judiciary Committee for study. It is unclear at this time whether or not this bill will be enacted. However, if it is, it is possible that the Committee will decide that continued investigation into the original program and its legality has become moot and will cease its investigation into both matters.

With respect to the NSA warrantless surveillance program in its current form, the President's Executive Order appears to permit the NSA to conduct a type of surveillance for the purpose of gathering signals intelligence similar to the type that Canada's CSE may, in certain circumstances, be authorized to carry out under section 273.65 of the *National Defence Act*.(47)

---

(46) The text of Bill S. 2455 is available on the Library of Congress' Web site at: http://thomas.loc.gov/.

(47) R.S.C. 1985, c. N-5.

There are, however, some important differences between the Canadian and U.S. approaches to warrantless surveillance by their respective signals intelligence agencies. Firstly, although the authorizations to intercept private communication that the Minister of National Defence may grant to the CSE under section 273.65 are exempt from publication requirements under the *Statutory Instruments Act*,(48) and thus, like President Bush's Executive Order, may be made secretly, the fact that the Minister may authorize such interceptions is not secret. It is, on the contrary, outlined in legislation. Secondly, Parliament enacted the legislative provisions authorizing the Minister to issue such authorizations to the CSE, in contrast to the situation in the United States, where, until recently, only select members of Congress were aware that the President had signed an Executive Order allowing the NSA to intercept communication beginning or terminating in the United States without need for prior judicial authorization. Finally, in the case of the CSE, the Minister's authority to authorize the CSE to intercept private communication is subject to certain legislative safeguards. He or she may authorize the interception of private communication only in certain specified circumstances and, in the event of interception, is required to ensure satisfactory measures are in place to protect the privacy of Canadians. It is unknown what, if any, restrictions on interception are contained in the President's Executive Order, as its contents remain secret.

INFORMATION GATHERING, SECRECY AND SHARING

The *Anti-terrorism Act* has done little to augment the federal government's power to gather and share information. It has, however, greatly enhanced the government's capacity to keep certain types of special information related to national security, international relations or national defence out of the hands of the public. For example, sections 38.13(1), (7), (8), (9) and 38.131 of the *Canada Evidence Act*, sections introduced into that Act by section 43 of the *Anti-terrorism Act*, provide that where a decision or order has been made under the *Canada Evidence Act* or any other Act of Parliament that would result in the disclosure of information, the Attorney General of Canada may issue a certificate prohibiting the disclosure of this information for the purpose of protecting information obtained in confidence from or in relation to a foreign entity or for the purpose of protecting national defence or national security. The

(48) R.S.C. 1985, c. S-22. The exemption from publication is contained in section 273.65(7) of the *National Defence Act.*

certificate must be published in the *Canada Gazette* and is valid for 15 years, unless reissued. A person who is party to the proceedings in relation to the certificate may seek a review of the Attorney General's decision to issue the certificate by a single judge of the Federal Court of Appeal, who is empowered to vary, confirm or cancel the certificate. There is no appeal available from the judge's decision.

Other examples of legislative changes introduced by the *Anti-terrorism Act* which have augmented the government's ability to have certain information kept secret or out of the hands of the person concerned are the *ex parte* and *in camera* hearings that the Minister of Public Safety and Emergency Preparedness, in the case of terrorist entities, or the Minister of Public Safety and Emergency Preparedness and the Minister of National Revenue, in the case of applicants for status as registered charities under the *Income Tax Act* or charities already registered under that Act,(49) may ask the Federal Court to hold when a judge of that court reviews the decisions of these Ministers to certify an entity as a terrorist entity, to deny an applicant status as a registered charity or to de-register a registered charity.(50) Before a judge will consent to a hearing in the absence of the person concerned and his or her counsel, the judge must be satisfied that disclosure of the information would injure national security or endanger the safety of any person. If the judge decides to hold a hearing in the absence of the person concerned and his or her counsel, the judge must still provide the person with a summary of the information available to the court and provide the applicant with a reasonable opportunity to be heard.

In contrast, amendments to the U.S.C. introduced by the Patriot Act 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.(51)

---

(49) R.S.C. 1985, c.1 (5th Supp.).

(50) See sections 83.05(6) and 83.06 of the *Criminal Code*, which were added to the Code by section 4 of the *Anti-terrorism Act* and section 6 of the *Charities Registration (Security Information) Act*, S.C. 2001, c. 41, an Act created by section 113 of the *Anti-terrorism Act.*

(51) Having said this, some sections of the Patriot Act are concerned with information secrecy. One example is the Act's 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.

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 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.(52)

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

---

(52) 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 on-line at: http://www.oipcbc.org/sector_public/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 and available on-line at http://www.privcom.gc.ca/media/nr-c/2004/sub_usapa_040818_e.pdf.

against international terrorism or clandestine intelligence activities.(53) 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. It is unclear at this time whether section 505, in particular, will pass U.S. constitutional muster. There are two U.S. District Federal Court decisions, one which states that section 505 violates the 1st (freedom of speech) and 4th (protection from unreasonable search and seizure) Amendments of the U.S. Constitution, and another which states that the automatic gag order under section 505,(54) which prohibits third parties from disclosing that they have received an NSL, violates the 1st Amendment.(55) Appeals of these cases were heard together by the Federal Appeals Court, 2nd Circuit, in November 2005. No decision has yet been rendered on these appeals.

LISTING OF TERRORIST ENTITIES

Canada's *Anti-terrorism Act* introduced a procedure for the listing of terrorist entities under the *Criminal Code*.(56) It is not an offence to be a listed entity in Canada; however, becoming a listed entity under the *Criminal Code* can have serious consequences, because listing means that the entity is automatically defined as a terrorist group, and those who associate with terrorist groups in certain ways are vulnerable to being charged under new *Criminal Code* provisions also introduced by the Act.(57) Thus, the effect of listing is to make it risky under the law for anyone to deal with the entity in question. In addition to adding offences to the *Criminal Code* designed to prohibit people from dealing with terrorist groups generally, the Act also

(53) See 18 U.S.C. 2709.

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

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

(56) See sections 83.05 to 83.07 of the *Criminal Code*, introduced into the Code by section 4 of the *Anti-terrorism Act*. In order to be placed on the list, the Governor in Council, on the recommendation of the Minister of Public Safety and Emergency Preparedness, must be satisfied that there are reasonable grounds to believe that the entity (which is defined to include an individual) has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity or that the entity is knowingly acting on behalf of, at the direction of or in association with an entity that has done so.

(57) See, for example, section 83.18 (prohibiting participation in the activity of a terrorist group), section 83.2 (prohibiting commission of an indictable offence at the direction of or in association with a terrorist group), and section 83.21 (prohibiting the direct or indirect carrying out of an activity for the benefit of a terrorist group) of the Code. All of these provisions were introduced into the Code by section 4 of the *Anti-terrorism Act*.

introduced offences designed discourage, deter and prohibit individuals and organizations from dealing with property belonging to terrorist groups,(58) providing or making available property or services for terrorist activities,(59) or collecting, providing, using or possessing property for terrorist activities,(60) regardless of whether these individuals and organizations are members of terrorist groups or not. Finally, the Act introduced *Criminal Code* provisions to permit the freezing and forfeiture of terrorist property.(61)

A similar listing process to the one in Canada's *Criminal Code* was introduced in the United States shortly after 11 September 2001. However, it was introduced not through the Patriot Act but instead by means of an Executive Order, E.O. 13224, signed by the President.(62) 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 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

---

(58) For example, see sections 83.08, 83.1 and 83.11 of the Code. Section 83.12 makes it an offence, punishable on summary conviction by a fine of not more than $100,000 or one year's imprisonment or both, or punishable on indictment by a term of imprisonment of not more than 10 years, to contravene sections 83.08, 83.1 of 83.11 of the Code.

(59) Section 83.03 of the Code makes providing or making available property or services for terrorist activities an indictable offence punishable by up to 10 years' imprisonment.

(60) Section 83.01 of the Code makes it an indictable offence punishable by up to 10 years' imprisonment to collect or provide property for terrorist or certain other activities, while section 83.04 makes it an indictable offence also punishable by up to 10 years' imprisonment to use or possess property for terrorist activities.

(61) For example, see section 83.13 of the Code, which allows the Federal Court to issue seizure or restraint orders for property owned or controlled by a terrorist group or property that will be used to facilitate or carry out a terrorist activity. With respect to forfeiture, section 83.14 of the Code allows the Attorney General to apply to the Federal Court for a forfeiture order respecting property, currency or monetary instruments controlled by individuals who have facilitated or carried out terrorist activities or are planning to do so. If the judge issues a forfeiture order, the property is forfeited to Her Majesty to be disposed of as the Attorney General directs or otherwise dealt with in accordance with the law.

(62) 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. To view the full text of E.O. 13224, please see the U.S. State Department's Web site at: http://www.state.gov/s/ct/rls/fs/2002/16181.htm.

attempt to evade a blocking order made by the Office of Foreign Asset Control (OFAC) of the Department of the Treasury.(63) Those who violate the prohibitions contained in E.O. 13224 may be subject to civil or criminal penalties.(64)

With respect to freezing and forfeiture provisions, the Patriot Act did introduce new forfeiture provisions specifically related to terrorism.(65) 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.(66)

SUPPRESSION OF TERRORIST FINANCING

The *Anti-terrorism Act* amended the *Proceeds of Crime (Money Laundering) Act*, changing its name to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA).(67) The PCMLTFA, in its original form, created a scheme that allowed for the monitoring and analysis of large and/or suspicious financial transactions that could be the proceeds of crime or money laundering. The *Anti-terrorism Act* made this scheme applicable to suspected terrorist financing activity as well as money laundering activity. In addition, the *Anti-terrorism Act* created a new statute, the *Charities Registration (Security Information) Act* (CRSIA),(68) which established a process through which organizations can lose or be denied tax advantages under the *Income Tax Act* if there are reasonable grounds to believe that they have made, or will make, resources available to a terrorist entity.

---

(63) 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.

(64) 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.

(65) See, for example, sections 106 and 806 of the Patriot Act.

(66) 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. 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.

(67) S.C. 2000, c. 17.

(68) S.C. 2001, c. 41.

By contrast, the Patriot Act did not introduce amendments to make the existing U.S. legislative scheme dealing with money laundering specifically applicable to terrorist financing offences. This is likely because the definition of money laundering under U.S. law prior to the enactment of the Patriot Act was broad enough to encompass terrorist activity.(69) 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.(70) With respect to the impact of the Patriot Act on charities, there does not appear to be an equivalent to the CRSIA in the United States.

SUNSET AND REVIEW PROVISIONS UNDER THE *ANTI-TERRORISM ACT*

Under the *Anti-terrorism Act*, the only provisions subject to sunset clauses are those related to investigative hearings and preventive arrests (sections 83.28, 83.29 and 83.3 of the *Criminal Code*). Pursuant to section 83.32 of the Code (also introduced into the Code by the Act), these provisions will expire on 31 December 2006 unless extended by resolutions of both Houses of Parliament.

However, section 145 of the Act required a committee of the Senate, the House of Commons or both, or a joint committee of both Houses of Parliament, to be designated or established to undertake a comprehensive review of the provisions and operation of the Act within three years of the date it received Royal Assent. The committee or committees established were also required to submit a report on the review to Parliament within a year of the review's being undertaken or within such further time as may be authorized by Parliament.

The *Anti-terrorism Act* received Royal Assent on 18 December 2001. On 9 December 2004, the House of Commons directed its Standing Committee on Justice, Human Rights, Public Safety and Emergency Preparedness, by order of reference, to undertake the review required by section 145 of the Act. The Committee subsequently delegated this task to one of its subcommittees, the Subcommittee on Public Safety and National Security. Following this, on 13 December 2004, the Senate, by order of reference, directed that a new committee, the

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

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

Special Senate Committee on the *Anti-terrorism Act*, be created and that it undertake the review required by section 145 of the Act. The Senate Special Committee commenced its review on 15 December 2004, and the House of Commons Subcommittee commenced its review on 16 December 2004. These two committees were engaged in conducting parallel reviews of the Act when Parliament was dissolved in November 2005.

SUNSET PROVISIONS UNDER THE PATRIOT ACT

In contrast to the *Anti-terrorism Act*, the Patriot Act contains 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[(71)] and the U.S. House of Representatives Committee on the Judiciary (the House Judiciary Committee).[(72)] Following study by these committees, the House of Representatives and the Senate each introduced its own reauthorization bill.[(73)] After much

(71) For more information on the review hearings conducted by the Senate Judiciary Committee respecting the Patriot Act, please see the Committee's Web site at: http://judiciary.senate.gov/search_testimony.cfm?testimony=Patriot+Act&Submit2=Submit.

(72) For more information on the review hearings conducted by the House Judiciary Committee respecting the Patriot Act, please see the Committee's Web site at: http://judiciary.house.gov/.

(73) 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' Web site at: http://www.fas.org/sgp/crs/intel/RL33027.pdf.

debate, two short extensions of all Patriot Act provisions scheduled to sunset on 31 December 2005,[74] and a conference committee report[75] that attempted to reconcile differences between the House and Senate bills, Congress eventually passed H.R. 3199, the USA PATRIOT Improvement and Reauthorization Act of 2005 (the Patriot Reauthorization Act or PRA).[76] 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).[77] Both bills were signed into law by the President on 9 March 2006.

THE PATRIOT REAUTHORIZATION ACT

The Patriot Reauthorization Act is a complex and comprehensive statute. It amended many provisions of the Patriot Act, introduced novel provisions and brought into force new pieces of legislation related to terrorism, such as the Combating Terrorism Financing Act of 2005[78] and the Reducing Crime and Terrorism at America's Seaports Act of 2005.[79] It also brought into force a new piece of legislation entirely unrelated to terrorism or national security,

---

(74) 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 (IRTPA) to July 1, 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.

(75) 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 is available on the Library of Congress' Web site 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' Web site at: http://www.fas.org/sgp/crs/intel/RL33239.pdf.

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

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

(78) This Act is found at Title IV, sections 401 to 410, of the PRA.

(79) This Act is found at Title III, sections 301 to 306, of the PRA.

the Combat Methamphetamine Epidemic Act of 2005.(80) A thorough review of the PRA is accordingly beyond the scope of this paper.(81)

With respect to the key changes or amendments that the PRA made to the Patriot Act, one of the most significant was that it made 14 of the 16 Patriot Act provisions originally destined to sunset on 31 December 2005 permanent. Among the provisions made permanent were sections 203(b), 203(d) and 218 of the Patriot Act, which were discussed earlier in this paper.(82) 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.(83)

In addition to extending the expiry dates for sections 206 (orders for roving FISA wiretaps) and 215 (production orders under FISA for access to tangible items) to 31 December 2009, the PRA amended these sections of the Patriot Act to increase procedural protections available to those affected by these orders and to make the tests for obtaining surveillance and production orders from the FISA court more stringent.

With respect to section 215 of the Patriot Act, the PRA introduced several significant amendments. Prior to the coming into force of the PRA, for example, any designee of the Director of the FBI, as long as his/her rank was no lower than Assistant Special Agent in Charge, could apply to the FISA court for a section 215 tangible items production order.

---

(80) This Act is found at Title VII, sections 701 and 711, of the PRA.

(81) For a thorough overview of the PRA, please see Charles Doyle and Brian T. Yeh, *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis*, Congressional Research Service, Washington, D.C., 24 March 2006, available on the Federation of American Scientists' Web site at: http://www.fas.org/sgp/crs/intel/RL33332.pdf.

(82) The other 11 Patriot Act sunset provisions which were made permanent by the PRA were sections 201 (authority for court-supervised wiretapping in cases involving various terrorism offences), 202 (authority for court-supervised wiretapping in computer fraud and abuse felony cases), 204 (clarification of intelligence exceptions to limitations placed on interception and disclosure of wire, oral and electronic communications), 207 (extended duration of FISA surveillance and physical search orders), 209 (authority for seizure of unopened voice-mail messages pursuant to search warrants), 212 (authority for emergency disclosure of customer communication records by Internet service providers), 214 (authority under FISA to use pen register/trap and trace devices to intercept e-mail and other Internet communications), 217 (authority to intercept the communications of computer trespassers without warrant or court order), 220 (authority for nationwide service of court orders for electronic surveillance), 223 (ability to sue the United States for willful violations of Title III or FISA by United States government officials) and 225 (immunity for those who aid federal officials to execute FISA surveillance or search orders or in the performance of emergency FISA wiretaps or searches).

(83) See section 102 of the PRA.

Section 106(a)(2) of the PRA restricted who was authorized to apply for such orders, at least with respect to orders sought for specific types of records. Section 106(a)(2) of the PRA states that if the section 215 tangible items production order being applied for is for certain types of sensitive records, such as library, tax return, educational or medical records, the application must be made by the FBI Director, FBI Deputy Director or Executive Assistant Director for National Security. Another amendment introduced by the PRA concerns documentation required for the section 215 application. Prior to enactment of the PRA, the FBI, when requesting a section 215 order, needed only to state in its application that the requested records were sought for an authorized investigation. Section 106(b)(2)(A) of the PRA amended this requirement to make it more stringent. Now, when applying for such an order, the FBI is required to submit a statement of facts that demonstrates there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against terrorism or espionage. Section 106(f) of the PRA also established a process by which recipients of a section 215 order wishing to challenge its legality might apply to the FISA court for judicial review of the order. A judge of that court is empowered to modify or set the order aside if he or she finds it does not comply with FISA or is otherwise unlawful. In addition, section 106 of the PRA clarifies that, while recipients of section 215 orders are still generally prohibited from disclosing that they have received one, recipients are allowed to inform their lawyers of this fact for the purpose of obtaining legal advice. They are not, however, able to apply for judicial review of the non-disclosure aspect of a section 215 order by virtue of this section of the PRA. Finally, section 106 of the PRA provides for enhanced congressional oversight over the use of section 215 of the Patriot Act by imposing more detailed reporting requirements on the Attorney General with respect to the use of this provision.

With respect to section 206 of the Patriot Act (roving FISA wiretaps), section 108 of the PRA amended the application process to add new procedural requirements. Section 108 also enhanced judicial and congressional oversight over these types of wiretap orders. Prior to the enactment of the PRA, when the identity of a section 206 roving surveillance target was unknown, it was sufficient for the order to describe the target. Section 108 of the PRA modified this requirement, making it mandatory for the application for the section 206 order, as well as the wiretap order itself, to describe the *specific* target of the surveillance. In addition, section 108 states that before granting a section 206 roving wiretap order, the FISA court must be satisfied

that specific facts in the application support the claim that the actions of target may have the effect of thwarting surveillance. Section 108 further states that, within 10 days of directing surveillance under section 206 at a new facility or place, the government must notify the FISA court of certain specified facts. Finally, section 108 of the PRA added the Senate Judiciary Committee to the list of House and Senate committees to which the Attorney General must submit semi-annual FISA reports and made it mandatory for the Attorney General to include a description of the number of applications made for section 206 roving surveillance orders in his/her FISA reports.

Other significant amendments that the PRA introduced into the Patriot Act are those found in sections 114 to 116 of the PRA. Section 114 of the PRA amends section 213 of the Patriot Act, the section that allows law enforcement officers to apply for and obtain "sneak and peak" warrants. Prior to the enactment of the PRA, those whose premises were searched under the authority of a "sneak and peak" warrant were required to be notified of the search within a reasonable time. The term "reasonable time" was not, however, defined. Now, under section 114 of the PRA, those whose premises are searched under authority of a warrant issued under section 213 of the Patriot Act are required to be notified of the warrant's execution no more than 30 days after it was executed. It is possible to obtain extensions of the delay period for up to 90 days if good cause is shown, and to obtain further extensions of up to 90 days if circumstances warrant.

Sections 115 and 116 of the PRA concern National Security Letters (NSLs). Section 115 of the PRA now allows recipients of NSLs to apply for judicial review of the decision to issue an NSL to a United States federal district court. This court is empowered to modify or quash the NSL if satisfied that compliance would be unreasonable, oppressive or otherwise unlawful. In addition, in contrast to the situation respecting section 215 tangible items search orders under section 106 of the PRA, recipients of NSLs are entitled to apply for judicial review of the non-disclosure aspect of the NSL. The reviewing judge may set aside the non-disclosure or "gag" aspect of the order if he/she finds no reason to believe that disclosure may endanger the security of the United States, interfere with a criminal, counterterrorism or counterintelligence investigation, interfere with diplomatic relations or endanger the life or physical safety of any person. If, however, at the time of the review, one of a list of specified government officials certifies that revealing the fact that such a letter has been issued may endanger the national security of the United States or interfere with diplomatic relations, such

certification shall be treated as conclusive by the reviewing judge, unless he or she finds that the certification was made in bad faith. The judicial review available with respect to the non-disclosure aspect of NSLs is, accordingly, limited. Section 116 of the PRA allows recipients of NSLs to disclose the fact that the FBI has sought or obtained access to information from them through an NSL to persons whose assistance is needed in order for the recipients to comply with the NSL or to their lawyers, for the purpose of obtaining legal advice or assistance with respect to the NSL.

As stated previously, the PRA amended many other sections of the Patriot Act. The amendments described above are simply some of the most significant ones.

THE ADDITIONAL REAUTHORIZING AMENDMENTS ACT

In addition to the PRA, the United States also enacted the ARAA.(84) The ARAA was enacted in response to the concerns expressed by various members of the House of Representatives and the Senate that the procedural protections available to recipients of section 215 tangible items orders and NSLs under the Patriot Act and the PRA were insufficient. These members were able to convince both Houses of Congress and the President that further changes were warranted.

One of the biggest criticisms some members had of the changes introduced by the PRA is that while the PRA allowed recipients of section 215 tangible item production orders to apply for judicial review of the decision to issue an order, no judicial review was available for the non-disclosure aspect of the order. Section 3 of the ARAA further amended section 215 of the Patriot Act to allow recipients of orders under this section to apply for judicial review of the secrecy or non-disclosure requirement. The test that must be satisfied in order for the judge to modify or set aside the non-disclosure requirement is the same as the one outlined in section 115 of the PRA for NSLs described above. The only difference is that a recipient can apply for judicial review of the non-disclosure aspect of a section 215 tangible item production order no sooner than one year after the order has been issued, whereas, in the case of NSLs, it is possible to apply for a review of the non-disclosure aspect of the letter before one year has elapsed, as well as after.

---

(84) For an overview of the ARAA, please see Brian T. Yeh, *USA Patriot Act Additional Reauthorizing Amendments Act of 2006*, Congressional Research Service, Washington, D.C., 21 February 2006, available on the Federation of American Scientists' Web site at: http://www.fas.org/sgp/crs/intel/RS22384.pdf.

With respect to NSLs, section 4 of the ARAA clarified that recipients of NSLs are not required to provide to the FBI the names of attorneys to whom they have disclosed the fact of receipt of an NSL in order to obtain legal advice. Moreover, section 5 of the ARAA clarified that libraries, when functioning in their traditional roles, including providing Internet access to their patrons, are not subject to NSLs as wire or electronic communication service providers. These latter two amendments were enacted to address concerns that recipients of NSLs, if required to provide the names of their lawyers to the FBI, might decide not to avail themselves of legal counsel, and to address concerns that libraries could be compelled to provide records of books borrowed and Internet records to the FBI through an NSL, which was viewed by many as a significant privacy violation.(85)

CONCLUSION

While Canada's *Anti-terrorism Act* and the United States' Patriot Act have similar goals, are directed at similar types of harm or activity, and are designed to give their governments new tools and powers so as to achieve their objectives, the tools and powers given to government officials by each statute are actually quite different. These differences reflect the fact that while Canada and the United States both have legal systems rooted in the British common law tradition, they, as sovereign nations, have developed different constitutional, legislative and bureaucratic structures, as well as somewhat different approaches to legislative problem solving.

---

(85) While the PRA dealt with the immediate issue of the Patriot Act sunset provisions, and the PRA and ARAA have introduced several procedural protections with respect to certain Patriot Act provisions, most notably sections 215 and 206 of the Patriot Act, some members of Congress appear unconvinced that the amendments have gone far enough. On 3 March 2006, Bill S. 2369, A bill to require a more reasonable period for delayed-notice search warrants, to provide enhanced judicial review of FISA orders and national security letters, to require an enhanced factual basis for a FISA order, and to create national security letter sunset provisions, was introduced in the Senate and referred to the Senate Judiciary Committee for further study. The title of the bill is indicative of the types of changes it is intended to introduce. If enacted, this bill would introduce additional procedural protections respecting "sneak and peek" warrants (section 213 of the Patriot Act), tangible items production orders (section 215 of the Patriot Act) and NSLs (sections 358 and 505 of the Patriot Act). The full text of the bill is available on the Library of Congress' Web site at: http://thomas.loc.gov.