Reference Materials with reference to Item 10 of the Explanatory Notes about the CSAs proposed by Hon. Margaret Ng

USA PATRIOT Act, Title II

From Wikipedia, the free encyclopedia

USA PATRIOT Act Titles
Title I: Enhancing Domestic Security against Terrorism
Title II: **Enhanced Surveillance Procedures**
Title III: International Money Laundering Abatement and Anti-terrorist Financing Act of 2001
Title IV: Protecting the border
Title V: Removing obstacles to investigating terrorism
Title VI: Providing for victims of terrorism, public safety officers and their families
Title VII: Increased information sharing for critical infrastructure protection
Title VIII: Strengthening the criminal laws against terrorism
Title IX: Improved intelligence
Title X: Miscellaneous

The USA PATRIOT Act was passed by the United States Congress in 2001 as a response to the September 11, 2001 attacks. It has ten titles, each containing numerous sections. **Title II: Enhanced Surveillance Procedures** granted increased powers of surveillance to various government agencies and bodies. This title has 25 sections, with one of the sections (section 224) containing a sunset clause which sets an expiration date, 31 December 2005, for most of the title's provisions. This was extended twice: on 22 December 2005 the sunset clause expiration date was extended to 3 February 2006 and on 2 February of the same year it was again extended, this time to March 10.

Title II contains many of the most contentious provisions of the act. Supporters of the Patriot Act claim that these provisions are necessary in fighting the War on Terrorism, while its detractors argue that many of the sections of Title II infringe upon individual and civil rights.

The sections of Title II amend the Foreign Intelligence Surveillance Act of 1978 and its provisions in 18 U.S.C., dealing with "Crimes and Criminal Procedure". It also amends the Electronic Communications Privacy Act of 1986. In general, the Title expands federal agencies' powers in intercepting, sharing, and using private telecommunications, especially electronic communications, along with a focus on criminal investigations by updating the rules that govern computer crime investigations. It also sets out procedures and limitations for individuals who feel their rights have been violated to seek redress, including against the United States government. However, it also includes a section that deals with trade sanctions against countries whose government supports terrorism, which is not directly related to surveillance issues.

Contents

Overview

Title II covers all aspects of the surveillance of suspected terrorists, those suspected of engaging in computer fraud or abuse, and agents of a foreign power who are engaged in clandestine activities (in other words, spying). In particular, the title allows government agencies to gather "foreign intelligence information" from both U.S. and non-U.S. citizens, which is defined in section 203 of the title. Section 218 changed the reason changed FISA to make "[the] *significant purpose* of the surveillance is to obtain foreign intelligence information" (change in italics). The change in definition was meant to remove a legal "wall" between criminal investigations and surveillance for the purposes of gathering foreign intelligence, which hampered investigations when criminal and foreign surveillance overlapped. However, that this wall even existed was found by the Federal Surveillance Court of Review to have actually been a long-held misinterpretation by government agencies. Section 203 also gave authorities the ability to share information gathered before a federal grand jury with other agencies.

Though not related to surveillance, the title also covers trade sanctions against the Taliban — which were determined by the Secretary of State to have repeatedly provided support for acts of international terrorism — and the export of agricultural commodities, medicine, or medical devices is now pursuant to one-year licenses issued and reviewed by the United States Government. It also excluded export of agricultural commodities, medicine, or medical devices to the Government of Syria and to the Government of North Korea.

Scope of allowed surveillance

The title allows surveillance to intercept communications via pen register or trap and trace devices. It does not allow these surveillance measures to be used in violation of the First Amendment rights of U.S. citizens. To assist in an investigation undertaken to protect against international terrorism or clandestine intelligence activities, the title allows for the seizure of communications records (section 215) and any records of session times, durations of electronic communication as well as any identifying numbers or addresses of the equipment that was being used (section 210). Such orders may be granted *ex parte*, and once they are granted — in order to not jeopardize the investigation — the order may not disclose the reasons behind why the order was granted. Section 209 made it easier for authorities to gain access to voicemail: they no longer must apply for a wiretap order, and instead just apply for a normal search warrant.

All orders granted under section 215 must be disclosed to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate. Every six months, the Attorney General must also provide a report to the Committees on the Judiciary of the House of Representatives and the Senate which details the total number of applications made for orders approving requests for the production of tangible things and the total number of such orders either granted, modified, or denied.

Under section 211, the United States Code was amended to allow the government to have access to the records of cable customers, with the notable exclusion of access to records revealing cable subscriber selection of video programming from a cable operator.

Disclosure

Section 212 stopped a communications provider from disclosing the contents of communications with another party. However, if the provider "reasonably" (not defined) believes that an emergency involving immediate danger of death or serious physical injury to any person is imminent, then the communications provider can now disclose this information without fear of legal liability. The provider may also disclose communications at the request of a government agency, if the customer allows it to be disclosed, or in cases where they must do so to protect their rights or property. Section 212 was later repealed by the Homeland Security Act of 2002 and was replaced with a new and permanent emergency disclosure provision.

Surveillance orders

In order for surveillance to be carried out, the United States Attorney General or his subordinates (so designated under section 201) may authorise a Federal judge to grant a surveillance order to the FBI or other Federal agency. Each of the orders granted must be reviewed by one of eleven District Court judges, of which at any one time three must live within 20 miles of the District of Columbia (see section 208).

Title II amended the US Code to allow a magistrate judge to issue a warrant outside of their district for any orders that relate to terrorism (section 219). Section 220 of the title also gave a Federal court judge the power to issue nationwide service of search warrants for electronic surveillance.

Under FISA, any agency may require a common carrier, landlord, custodian, or other person provide them with all information, facilities, or technical assistance necessary to accomplish ongoing electronic surveillance. They must also protect the secrecy of and cause as little disruption to the ongoing surveillance effort as possible. This was further tighted in section 206. Section 222 further limited the sort of assistance an agency may require, and provided for compensation of any person who rendered surveillance assistance to the government agency. Section 225 allows for legal immunity to any provider of a wire or electronic communication service, landlord, custodian, or other person that provides any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance

Liability due to unauthorised surveillance

Section 223 allows any party who has had their rights violated due to the illegal interception of communications to take civil action against those who undertook the illegal surveillance.

Sunset

This article or section needs to be updated.
Parts of this article or section have been identified as no longer being up to date.

Please update the article to reflect recent events, and remove this template when finished.

Section 224 (*Sunset*) is a sunset clause. Title II and the amendments made by the title originally would have ceased to have effect on December 31, 2005, with the exception of the below sections. However, on December 22, 2005, the sunset clause expiration date was extended to February 3, 2006, and then on February 2, 2006 it was further extended to March 10:

Title II sections that will **not** expire on March 10, 2006

Section	Section title
203(a)	Authority to share criminal investigation information : Authority to share Grand Jury information
203(c)	Authority to share criminal investigation information : Procedures
205	Employment of translators by the Federal Bureau of Investigation
208	Designation of judges
210	Scope of subpoenas for records of electronic communications
211	Clarification of scope
213	Authority for delaying notice of the execution of a warrant
216	Modification of authorities relating to use of pen registers and

President George W. Bush addresses an audience Wednesday, July 20, 2005 at the Port of Baltimore in Baltimore, Md., encouraging the renewal of provisions of the Patriot Act.

	trap and trace devices
219	Single-jurisdiction search warrants for terrorism
221	Trade sanctions
222	Assistance to law enforcement agencies

Further, any particular foreign intelligence investigations that are ongoing will continue to be run under the expired sections.

5

USA PATRIOT Act

Under §224 of the USA PATRIOT Act several of the surveillance portions originally expired on December 31, 2005 [1], these have since been renewed, but has expired on March 10, 2006. The USA PATRIOT Act is set to sunset the following provisions:

- §201 Wiretapping for terrorism cases
- §202 Wiretapping for computer fraud and abuse
- §203(b) and (d) Sharing of wiretap and foreign intelligence information
- §§204, 206, 207, 214, 215, 218, and 225 Foreign Intelligence Surveillance Act related sections including roving wiretaps
- §209 Warranted seizure of voicemail messages
- §217 Computer trespasser communications
- §220 Nationwide service or warrants for electronic evidence
- §223 Privacy violation civil liability

6

Patriot Act

"(C) when the United States is engaged in armed hostilities or has been attacked by a foreign country or foreign nationals, confiscate any property, subject to the jurisdiction of the United States, of any foreign person, foreign organization, or foreign country that he determines has planned, authorized, aided, or engaged in such hostilities or attacks against the United States; and all right, title, and interest in any property so confiscated shall vest, when, as, and upon the terms directed by the President, in such agency or person as the President may designate from time to time, and upon such terms and conditions as the President may prescribe, such interest or property shall be held, used, administered, liquidated, sold, or otherwise dealt with in the interest of and for the benefit of the United States, and such designated agency or person may perform any and all acts incident to the accomplishment or furtherance of these purposes."; and

(2) by inserting at the end the following:

"(c) CLASSIFIED INFORMATION.—In any judicial review of a determination made under this section, if the determination was based on classified information (as defined in section 1(a) of the Classified Information Procedures Act) such information may be submitted to the reviewing court ex parte and in camera. This subsection does not confer or imply any right to judicial review.".

TITLE II—ENHANCED SURVEILLANCE PROCEDURES

SEC. 201. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO TERRORISM.

Section 2516(1) of title 18, United States Code, is amended—

(1) by redesignating paragraph (p), as so redesignated by section 434(2) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104–132; 110 Stat. 1274), as paragraph (r); and

(2) by inserting after paragraph (p), as so redesignated by section 201(3) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (division C of Public Law 104–208; 110 Stat. 3009–565), the following new paragraph:

"(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism); or".

SEC. 202. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO COMPUTER FRAUD AND ABUSE OFFENSES.

Section 2516(1)(c) of title 18, United States Code, is amended by striking "and section 1341 (relating to mail fraud)," and inserting "section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse),".

18 USC app.

SEC. 203. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION.

(a) AUTHORITY TO SHARE GRAND JURY INFORMATION.—

(1) IN GENERAL.—Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure is amended to read as follows:

"(C)(i) Disclosure otherwise prohibited by this rule of matters occurring before the grand jury may also be made—

"(I) when so directed by a court preliminarily to or in connection with a judicial proceeding;

"(II) when permitted by a court at the request of the defendant, upon a showing that grounds may exist for a motion to dismiss the indictment because of matters occurring before the grand jury;

"(III) when the disclosure is made by an attorney for the government to another Federal grand jury;

"(IV) when permitted by a court at the request of an attorney for the government, upon a showing that such matters may disclose a violation of State criminal law, to an appropriate official of a State or subdivision of a State for the purpose of enforcing such law; or

"(V) when the matters involve foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in clause (iv) of this subparagraph), to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.

"(ii) If the court orders disclosure of matters occurring before the grand jury, the disclosure shall be made in such manner, at such time, and under such conditions as the court may direct.

"(iii) Any Federal official to whom information is disclosed pursuant to clause (i)(V) of this subparagraph may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made.

"(iv) In clause (i)(V) of this subparagraph, the term 'foreign intelligence information' means—

"(I) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

"(aa) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

"(bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

"(cc) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of foreign power; or

9

"(II) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

"(aa) the national defense or the security of the United States; or

"(bb) the conduct of the foreign affairs of the United States.".

(2) CONFORMING AMENDMENT.—Rule 6(e)(3)(D) of the Federal Rules of Criminal Procedure is amended by striking "(e)(3)(C)(i)" and inserting "(e)(3)(C)(i)(I)".

(b) AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION.—

(1) LAW ENFORCEMENT.—Section 2517 of title 18, United States Code, is amended by inserting at the end the following:

"(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.".

(2) DEFINITION.—Section 2510 of title 18, United States Code, is amended by—

(A) in paragraph (17), by striking "and" after the semicolon;

(B) in paragraph (18), by striking the period and inserting "; and"; and

(C) by inserting at the end the following:

"(19) 'foreign intelligence information' means—

"(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

"(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

"(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

"(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

"(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

"(i) the national defense or the security of the United States; or

"(ii) the conduct of the foreign affairs of the United States.".

18 USC 2517 note.

(c) PROCEDURES.—The Attorney General shall establish procedures for the disclosure of information pursuant to section 2517(6) and Rule 6(e)(3)(C)(i)(V) of the Federal Rules of Criminal Procedure that identifies a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)).

50 USC 403–5d.

(d) FOREIGN INTELLIGENCE INFORMATION.—

(1) IN GENERAL.—Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(2) DEFINITION.—In this subsection, the term "foreign intelligence information" means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

SEC. 204. CLARIFICATION OF INTELLIGENCE EXCEPTIONS FROM LIMITATIONS ON INTERCEPTION AND DISCLOSURE OF WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS.

Section 2511(2)(f) of title 18, United States Code, is amended—

(1) by striking "this chapter or chapter 121" and inserting "this chapter or chapter 121 or 206 of this title"; and

(2) by striking "wire and oral" and inserting "wire, oral, and electronic".

SEC. 205. EMPLOYMENT OF TRANSLATORS BY THE FEDERAL BUREAU OF INVESTIGATION.

28 USC 532 note.

(a) AUTHORITY.—The Director of the Federal Bureau of Investigation is authorized to expedite the employment of personnel as translators to support counterterrorism investigations and operations without regard to applicable Federal personnel requirements and limitations.

(b) SECURITY REQUIREMENTS.—The Director of the Federal Bureau of Investigation shall establish such security requirements as are necessary for the personnel employed as translators under subsection (a).

(c) REPORT.—The Attorney General shall report to the Committees on the Judiciary of the House of Representatives and the Senate on—

(1) the number of translators employed by the FBI and other components of the Department of Justice;

(2) any legal or practical impediments to using translators employed by other Federal, State, or local agencies, on a full, part-time, or shared basis; and

(3) the needs of the FBI for specific translation services in certain languages, and recommendations for meeting those needs.

SEC. 206. ROVING SURVEILLANCE AUTHORITY UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by inserting ", or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons," after "specified person".

SEC. 207. DURATION OF FISA SURVEILLANCE OF NON-UNITED STATES PERSONS WHO ARE AGENTS OF A FOREIGN POWER.

(a) DURATION.—

(1) SURVEILLANCE.—Section 105(e)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(e)(1)) is amended by—

(A) inserting "(A)" after "except that"; and

(B) inserting before the period the following: ", and (B) an order under this Act for a surveillance targeted against an agent of a foreign power, as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less".

(2) PHYSICAL SEARCH.—Section 304(d)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(1)) is amended by—

(A) striking "forty-five" and inserting "90";

(B) inserting "(A)" after "except that"; and

(C) inserting before the period the following: ", and (B) an order under this section for a physical search targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less".

(b) EXTENSION.—

(1) IN GENERAL.—Section 105(d)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(d)(2)) is amended by—

(A) inserting "(A)" after "except that"; and

(B) inserting before the period the following: ", and (B) an extension of an order under this Act for a surveillance targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for a period not to exceed 1 year".

(2) DEFINED TERM.—Section 304(d)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(2)) is amended by inserting after "not a United States person," the following: "or against an agent of a foreign power as defined in section 101(b)(1)(A),".

SEC. 208. DESIGNATION OF JUDGES.

Section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)) is amended by—

(1) striking "seven district court judges" and inserting "11 district court judges"; and

(2) inserting "of whom no fewer than 3 shall reside within 20 miles of the District of Columbia" after "circuits".

SEC. 209. SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS.

Title 18, United States Code, is amended—

(1) in section 2510—

(A) in paragraph (1), by striking beginning with "and such" and all that follows through "communication"; and

(B) in paragraph (14), by inserting "wire or" after "transmission of"; and

(2) in subsections (a) and (b) of section 2703—

(A) by striking "CONTENTS OF ELECTRONIC" and inserting "CONTENTS OF WIRE OR ELECTRONIC" each place it appears;

(B) by striking "contents of an electronic" and inserting "contents of a wire or electronic" each place it appears; and

(C) by striking "any electronic" and inserting "any wire or electronic" each place it appears.

SEC. 210. SCOPE OF SUBPOENAS FOR RECORDS OF ELECTRONIC COMMUNICATIONS.

Section 2703(c)(2) of title 18, United States Code, as redesignated by section 212, is amended—

(1) by striking "entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber" and inserting the following: "entity the—

"(A) name;

"(B) address;

"(C) local and long distance telephone connection records, or records of session times and durations;

"(D) length of service (including start date) and types of service utilized;

"(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

"(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber"; and

(2) by striking "and the types of services the subscriber or customer utilized,".

SEC. 211. CLARIFICATION OF SCOPE.

Section 631 of the Communications Act of 1934 (47 U.S.C. 551) is amended—

(1) in subsection (c)(2)—

(A) in subparagraph (B), by striking "or";

(B) in subparagraph (C), by striking the period at the end and inserting "; or"; and

(C) by inserting at the end the following:

"(D) to a government entity as authorized under chapters 119, 121, or 206 of title 18, United States Code, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator."; and

(2) in subsection (h), by striking "A governmental entity" and inserting "Except as provided in subsection (c)(2)(D), a governmental entity".

SEC. 212. EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT LIFE AND LIMB.

(a) DISCLOSURE OF CONTENTS.—

(1) IN GENERAL.—Section 2702 of title 18, United States Code, is amended—

(A) by striking the section heading and inserting the following:

"§ 2702. Voluntary disclosure of customer communications or records";

(B) in subsection (a)—

(i) in paragraph (2)(A), by striking "and" at the end;

(ii) in paragraph (2)(B), by striking the period and inserting "; and"; and

(iii) by inserting after paragraph (2) the following:

"(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.";

(C) in subsection (b), by striking "EXCEPTIONS.—A person or entity" and inserting "EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.— A provider described in subsection (a)";

(D) in subsection (b)(6)—

(i) in subparagraph (A)(ii), by striking "or";

(ii) in subparagraph (B), by striking the period and inserting "; or"; and

(iii) by adding after subparagraph (B) the following:

"(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."; and

(E) by inserting after subsection (b) the following:

"(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.— A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

"(1) as otherwise authorized in section 2703;

"(2) with the lawful consent of the customer or subscriber;

"(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

"(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

"(5) to any person other than a governmental entity.".

(2) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2702 and inserting the following:

"2702. Voluntary disclosure of customer communications or records.".

(b) REQUIREMENTS FOR GOVERNMENT ACCESS.—

(1) IN GENERAL.—Section 2703 of title 18, United States Code, is amended—

(A) by striking the section heading and inserting the following:

"§ 2703. Required disclosure of customer communications or records";

(B) in subsection (c) by redesignating paragraph (2) as paragraph (3);

(C) in subsection (c)(1)—

(i) by striking "(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may" and inserting "A governmental entity may require a provider of electronic communication service or remote computing service to";

(ii) by striking "covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

"(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity" and inserting ")";

(iii) by redesignating subparagraph (C) as paragraph (2);

(iv) by redesignating clauses (i), (ii), (iii), and (iv) as subparagraphs (A), (B), (C), and (D), respectively;

(v) in subparagraph (D) (as redesignated) by striking the period and inserting "; or"; and

(vi) by inserting after subparagraph (D) (as redesignated) the following:

"(E) seeks information under paragraph (2).."; and

(D) in paragraph (2) (as redesignated) by striking "subparagraph (B)" and insert "paragraph (1)".

(2) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2703 and inserting the following:

"2703. Required disclosure of customer communications or records.".

SEC. 213. AUTHORITY FOR DELAYING NOTICE OF THE EXECUTION OF A WARRANT.

Section 3103a of title 18, United States Code, is amended—

(1) by inserting "(a) IN GENERAL.—" before "In addition"; and

(2) by adding at the end the following:

"(b) DELAY.—With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—

"(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);

"(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

"(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.".

SEC. 214. PEN REGISTER AND TRAP AND TRACE AUTHORITY UNDER FISA.

(a) APPLICATIONS AND ORDERS.—Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended—

(1) in subsection (a)(1), by striking "for any investigation to gather foreign intelligence information or information concerning international terrorism" and inserting "for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution";

(2) by amending subsection (c)(2) to read as follows:

"(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.";

(3) by striking subsection (c)(3); and

(4) by amending subsection (d)(2)(A) to read as follows:

"(A) shall specify—

"(i) the identity, if known, of the person who is the subject of the investigation;

"(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

"(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.".

(b) AUTHORIZATION DURING EMERGENCIES.—Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended—

(1) in subsection (a), by striking "foreign intelligence information or information concerning international terrorism" and inserting "foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution"; and

(2) in subsection (b)(1), by striking "foreign intelligence information or information concerning international terrorism" and inserting "foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution".

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

"SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS. 50 USC 1861.

"(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

"(2) An investigation conducted under this section shall—

"(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

"(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

"(b) Each application under this section—

"(1) shall be made to—

"(A) a judge of the court established by section 103(a); or

"(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

"(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

"(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

"(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

"(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

"(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

60 USC 1862.

"SEC. 502. CONGRESSIONAL OVERSIGHT.

"(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.

"(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

"(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and

"(2) the total number of such orders either granted, modified, or denied.".

SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) GENERAL LIMITATIONS.—Section 3121(c) of title 18, United States Code, is amended—

(1) by inserting "or trap and trace device" after "pen register";

(2) by inserting ", routing, addressing," after "dialing"; and

(3) by striking "call processing" and inserting "the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications".

(b) ISSUANCE OF ORDERS.—

(1) IN GENERAL.—Section 3123(a) of title 18, United States Code, is amended to read as follows:

"(a) IN GENERAL.—

"(1) ATTORNEY FOR THE GOVERNMENT.—Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

"(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

"(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify—

"(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

"(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

"(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

"(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

"(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).".

(2) CONTENTS OF ORDER.—Section 3123(b)(1) of title 18, United States Code, is amended—

(A) in subparagraph (A)—

(i) by inserting "or other facility" after "telephone line"; and

(ii) by inserting before the semicolon at the end "or applied"; and

(B) by striking subparagraph (C) and inserting the following:

"(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and".

(3) NONDISCLOSURE REQUIREMENTS.—Section 3123(d)(2) of title 18, United States Code, is amended—

(A) by inserting "or other facility" after "the line"; and

(B) by striking ", or who has been ordered by the court" and inserting "or applied, or who is obligated by the order".

(c) DEFINITIONS.—

(1) COURT OF COMPETENT JURISDICTION.—Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:

"(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or".

(2) PEN REGISTER.—Section 3127(3) of title 18, United States Code, is amended—

(A) by striking "electronic or other impulses" and all that follows through "is attached" and inserting "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication"; and

(B) by inserting "or process" after "device" each place it appears.

(3) TRAP AND TRACE DEVICE.—Section 3127(4) of title 18, United States Code, is amended—

(A) by striking "of an instrument" and all that follows through the semicolon and inserting "or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;"; and

(B) by inserting "or process" after "a device".

(4) CONFORMING AMENDMENT.—Section 3127(1) of title 18, United States Code, is amended—

(A) by striking "and"; and

(B) by inserting ", and 'contents'" after "electronic communication service".

(5) TECHNICAL AMENDMENT.—Section 3124(d) of title 18, United States Code, is amended by striking "the terms of".

(6) CONFORMING AMENDMENT.—Section 3124(b) of title 18, United States Code, is amended by inserting "or other facility" after "the appropriate line".

SEC. 217. INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS.

Chapter 119 of title 18, United States Code, is amended—

(1) in section 2510—

(A) in paragraph (18), by striking "and" at the end;

(B) in paragraph (19), by striking the period and inserting a semicolon; and

(C) by inserting after paragraph (19) the following:

"(20) 'protected computer' has the meaning set forth in section 1030; and

"(21) 'computer trespasser'—

"(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

"(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.";

(2) in section 2511(2), by inserting at the end the following:

"(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

"(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

"(II) the person acting under color of law is lawfully engaged in an investigation;

"(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

"(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.".

SEC. 218. FOREIGN INTELLIGENCE INFORMATION.

Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking "the purpose" and inserting "a significant purpose".

SEC. 219. SINGLE-JURISDICTION SEARCH WARRANTS FOR TERRORISM. 18 USC app.

Rule 41(a) of the Federal Rules of Criminal Procedure is amended by inserting after "executed" the following: "and (3) in an investigation of domestic terrorism or international terrorism (as defined in section 2331 of title 18, United States Code), by a Federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district".

SEC. 220. NATIONWIDE SERVICE OF SEARCH WARRANTS FOR ELECTRONIC EVIDENCE.

(a) IN GENERAL.—Chapter 121 of title 18, United States Code, is amended—

(1) in section 2703, by striking "under the Federal Rules of Criminal Procedure" every place it appears and inserting "using the procedures described in the Federal Rules of

Criminal Procedure by a court with jurisdiction over the offense under investigation"; and

(2) in section 2711—

(A) in paragraph (1), by striking "and";

(B) in paragraph (2), by striking the period and inserting "; and"; and

(C) by inserting at the end the following:

"(3) the term 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitations.".

(b) CONFORMING AMENDMENT.—Section 2703(d) of title 18, United States Code, is amended by striking "described in section 3127(2)(A)".

SEC. 221. TRADE SANCTIONS.

(a) IN GENERAL.—The Trade Sanctions Reform and Export Enhancement Act of 2000 (Public Law 106–387; 114 Stat. 1549A–67) is amended—

(1) by amending section 904(2)(C) to read as follows:

"(C) used to facilitate the design, development, or production of chemical or biological weapons, missiles, or weapons of mass destruction.";

(2) in section 906(a)(1)—

(A) by inserting ", the Taliban or the territory of Afghanistan controlled by the Taliban," after "Cuba"; and

(B) by inserting ", or in the territory of Afghanistan controlled by the Taliban," after "within such country"; and

(3) in section 906(a)(2), by inserting ", or to any other entity in Syria or North Korea" after "Korea".

22 USC 7210. (b) APPLICATION OF THE TRADE SANCTIONS REFORM AND EXPORT ENHANCEMENT ACT.—Nothing in the Trade Sanctions Reform and Export Enhancement Act of 2000 shall limit the application or scope of any law establishing criminal or civil penalties, including any Executive order or regulation promulgated pursuant to such laws (or similar or successor laws), for the unlawful export of any agricultural commodity, medicine, or medical device to—

(1) a foreign organization, group, or person designated pursuant to Executive Order No. 12947 of January 23, 1995, as amended;

(2) a Foreign Terrorist Organization pursuant to the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104–132);

(3) a foreign organization, group, or person designated pursuant to Executive Order No. 13224 (September 23, 2001);

(4) any narcotics trafficking entity designated pursuant to Executive Order No. 12978 (October 21, 1995) or the Foreign Narcotics Kingpin Designation Act (Public Law 106–120); or

(5) any foreign organization, group, or persons subject to any restriction for its involvement in weapons of mass destruction or missile proliferation.

18 USC 2518 note. SEC. 222. ASSISTANCE TO LAW ENFORCEMENT AGENCIES.

Nothing in this Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance. A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to section 216 shall be reasonably compensated for such reasonable expenditures incurred in providing such facilities or assistance.

SEC. 223. CIVIL LIABILITY FOR CERTAIN UNAUTHORIZED DISCLOSURES.

(a) Section 2520 of title 18, United States Code, is amended—

(1) in subsection (a), after "entity", by inserting ", other than the United States.";

(2) by adding at the end the following:

"(f) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination."; and

(3) by adding a new subsection (g), as follows:

"(g) IMPROPER DISCLOSURE IS VIOLATION.—Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).".

(b) Section 2707 of title 18, United States Code, is amended—

(1) in subsection (a), after "entity", by inserting ", other than the United States,";

(2) by striking subsection (d) and inserting the following:

"(d) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination."; and

(3) by adding a new subsection (g), as follows:

"(g) IMPROPER DISCLOSURE.—Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or

14

from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.".

(c)(1) Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

"§ 2712. Civil actions against the United States

"(a) IN GENERAL.—Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages—

"(1) actual damages, but not less than $10,000, whichever amount is greater; and

"(2) litigation costs, reasonably incurred.

"(b) PROCEDURES.—(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

"(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

"(3) Any action under this section shall be tried to the court without a jury.

"(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

"(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

"(c) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

"(d) EXCLUSIVE REMEDY.—Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

"(e) STAY OF PROCEEDINGS.—(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

"(2) In this subsection, the terms 'related criminal case' and 'related investigation' mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

"(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.".

(2) The table of sections at the beginning of chapter 121 is amended to read as follows:

"2712. Civil action against the United States.".

18 USC 2510 note.

SEC. 224. SUNSET.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.

(b) EXCEPTION.—With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

SEC. 225. IMMUNITY FOR COMPLIANCE WITH FISA WIRETAP.

Section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805) is amended by inserting after subsection (g) the following:

4

15

"(h) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act.".

International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001.
31 USC 5301 note.

TITLE III—INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001

SEC. 301. SHORT TITLE.

This title may be cited as the "International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001".

31 USC 5311 note.

SEC. 302. FINDINGS AND PURPOSES.

(a) FINDINGS.—The Congress finds that—

(1) money laundering, estimated by the International Monetary Fund to amount to between 2 and 5 percent of global gross domestic product, which is at least $600,000,000,000 annually, provides the financial fuel that permits transnational criminal enterprises to conduct and expand their operations to the detriment of the safety and security of American citizens;

(2) money laundering, and the defects in financial transparency on which money launderers rely, are critical to the financing of global terrorism and the provision of funds for terrorist attacks;

(3) money launderers subvert legitimate financial mechanisms and banking relationships by using them as protective covering for the movement of criminal proceeds and the financing of crime and terrorism, and, by so doing, can threaten the safety of United States citizens and undermine the integrity of United States financial institutions and of the global financial and trading systems upon which prosperity and growth depend;

(4) certain jurisdictions outside of the United States that offer "offshore" banking and related facilities designed to provide anonymity, coupled with weak financial supervisory and enforcement regimes, provide essential tools to disguise ownership and movement of criminal funds, derived from, or used to commit, offenses ranging from narcotics trafficking, terrorism, arms smuggling, and trafficking in human beings, to financial frauds that prey on law-abiding citizens;

(5) transactions involving such offshore jurisdictions make it difficult for law enforcement officials and regulators to follow the trail of money earned by criminals, organized international criminal enterprises, and global terrorist organizations;

(6) correspondent banking facilities are one of the banking mechanisms susceptible in some circumstances to manipulation by foreign banks to permit the laundering of funds by hiding the identity of real parties in interest to financial transactions;

(7) private banking services can be susceptible to manipulation by money launderers, for example corrupt foreign government officials, particularly if those services include the creation of offshore accounts and facilities for large personal funds transfers to channel funds into accounts around the globe;

15

3ZQP Matters to which documents must relate

A document to be produced under a notice under section 3ZQN or 3ZQO must relate to one or more of the following matters:

(a) determining whether an account is held by a specified person with a specified financial institution, and details relating to the account (including details of any related accounts);

(b) determining whether a specified person is a signatory to an account with a specified financial institution, and details relating to the account (including details of any related accounts);

(c) determining whether a transaction has been conducted by a specified financial institution on behalf of a specified person, and details relating to the transaction (including details relating to other parties to the transaction);

(d) determining whether a specified person travelled or will travel between specified dates or specified locations, and details relating to the travel (including details relating to other persons travelling with the specified person);

(e) determining whether assets have been transferred to or from a specified person between specified dates, and details relating to the transfers (including details relating to the names of any other persons to or from whom the assets were transferred);

(f) determining whether an account is held by a specified person in respect of a specified utility (such as gas, water or electricity), and details relating to the account (including the names of any other persons who also hold the account);

(g) determining who holds an account in respect of a specified utility (such as gas, water or electricity) at a specified place, and details relating to the account;

(h) determining whether a telephone account is held by a specified person, and details relating to the account (including:

(i) details in respect of calls made to or from the relevant telephone number; or

(ii) the times at which such calls were made or received; or

(iii) the lengths of such calls; or

(iv) the telephone numbers to which such calls were made and from which such calls were received);

(i) determining who holds a specified telephone account, and details relating to the account (including details mentioned in paragraph (h));

(j) determining whether a specified person resides at a specified place;

(k) determining who resides at a specified place.

3ZQQ Powers conferred on Federal Magistrates in their personal capacity

(1) A power conferred on a Federal Magistrate by section 3ZQO is conferred on the Magistrate in a personal capacity and not as a court or a member of a court.

(2) A Federal Magistrate need not accept the power conferred.

(3) A Federal Magistrate exercising a power conferred by section 3ZQO has the same protection and immunity as if he or she were exercising that power as, or as a member of, the court of which the Magistrate is a member.

3ZQR Documents must be produced

(1) A person is not excused from producing a document under section 3ZQN or 3ZQO on the ground that to do so:

(a) would contravene any other law; or

(b) might tend to incriminate the person or otherwise expose the person to a penalty or other liability; or

(c) would disclose material that is protected against disclosure by legal professional privilege or any other duty of confidence; or

(d) would be otherwise contrary to the public interest.

(2) However, neither:

(a) the production of the document; nor

(b) any information, document or thing obtained as a direct or indirect consequence of producing the document;

is admissible in evidence against the person in proceedings other than proceedings for an offence against section 137.1, 137.2 or 149.1 of the *Criminal Code* that relates to this Act.

(3) A person is not liable to any penalty by reason of his or her producing a document when required to do so under section 3ZQN or 3ZQO.

(4) The fact that a person is not excused under subsection (1) from producing a document does not otherwise affect a claim of legal professional privilege that anyone may make in relation to that document.

3ZQS Offence for failure to comply with notice under section 3ZQN or 3ZQO

A person commits an offence if:

(a) the person is given a notice under section 3ZQN or 3ZQO; and

(b) the person fails to comply with the notice.

Penalty: 30 penalty units.

3ZQT Offence for disclosing existence or nature of notice

(1) A person commits an offence if:

(a) the person is given a notice under section 3ZQN or 3ZQO; and

(b) the notice specifies that information about the notice must not be disclosed; and

(c) the person discloses the existence or nature of the notice.

Penalty: 120 penalty units or imprisonment for 2 years, or both.

(2) Subsection (1) does not apply if:

(a) the person discloses the information to another person in order to obtain a document that is required by the notice in order to comply with it, and that other person is directed not to inform the person to whom the document relates about the matter; or

(b) the disclosure is made to obtain legal advice or legal representation in relation to the notice; or

(c) the disclosure is made for the purposes of, or in the course of, legal proceedings.

Note: A defendant bears an evidential burden in relation to the matters in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

Law Council of Australia's report on Anti-Terrorism Bill (excerpts)

18

Reporting and Review

100. The Attorney General must prepare an annual report on the operation of laws relating to detention and control orders and table it in Parliament.

101. The Law Council suggests that yearly reports are inadequate. Regular reports on a quarterly or half yearly basis should be tabled in the Australian Parliament by the Attorney-General in relation to the application of the law, including the places and circumstances of detention. Information in the Annual Report should include the number of young persons aged 16-18 years and foreign nationals subject to orders made. The annual report should also indicate the number (and proportion) of persons subject to orders who were subsequently charged and convicted of terrorist related offences.

102. Further, as annual reporting is inadequate as a system of review, the Law Council believes that the operation of the Bill should be subjected to periodic statutory reviews of at least every 2 years (instead of 5 years).

103. The *Security Legislation Amendment (Terrorism) Act 2002* ("SLAT Act") and the review pursuant to the *Australian Crime Commission Act 2002* are required to occur after three years. The Law Council believes that a similar timeframe for such extreme laws as are found in the Bill is necessary.

104. The Law Council also notes that, as the sunset clause takes effect after 10 years, a review after 5 years appears inadequate in correcting problems and implementing change, where appropriate. The Law Council suggests that the review should be referred by Parliament to a suitably qualified person such as a former judge to conduct the inquiry and report. Alternatively, regular reviews which are similar to that provided under the SLAT Act are also appropriate. Law Council nominees should be appointed to any such review.

Operation of the Sunset Clause

105. According to the Bill, sunset clauses operate in relation to control orders and preventative detention orders and the

powers to stop, question and search persons in relation to terrorist acts in which these provisions cease to have effect after 10 years from the date of commencement (proposed s104.32 and s105.53) and in relation to certain police powers under the Crimes Act (proposed s3UK).

106. Should the recommendation made by the Law Council in relation to financing terrorism and sedition be ignored, the Law Council believes that the sunset clause should be extended to these provisions due to the over reach of the proposed law.

Law Council OF AUSTRALIA

Home
About Us
FAQ
For the Media
Policies and Guidelines
Publications
National Practice
Submissions
Sections
Conferences
Scholarships and Awards
Traineeships
Positions Vacant
Links
Search this Site
Site Map
Contacting Us
Members' Page
Privacy Policy

25 October 2005

Anti-Terror Bill: Judiciary Compromised

The version of the Anti-Terrorism Bill currently in the public domain contains major constitutional and procedural flaws which compromise the role of the Australian judiciary, said the Law Council today.

"In our constitutional system the separation of powers is paramount - the judiciary must remain independent of the Executive. Federal courts can only be asked to exercise judicial functions," said John North, President of the Law Council.

"Federal judges, even when not sitting in court, can't be asked to perform functions incompatible with judicial functions. These measures should not be allowed to pass into law," he said.

The power to make control orders is to be given to federal courts and is clearly non-judicial. Judicial power requires a fair procedure, including notice of the proceedings and disclosure of the basis upon which orders are sought and made. None of this occurs in relation to control orders.

The power to make detention orders is given to federal judicial officers in their personal capacity. To require them to make detention orders runs the grave risk of asking them to do tasks incompatible with their office.

Federal judicial officers are asked to make continued preventative detention orders following an initial order made by an AFP officer.

"Judicial officers will be exercising what is obviously a police function" a function of the Executive - and this will run the risk of prejudicing public confidence in the independence of the judiciary. State and Territory courts must ensure that their independence is preserved in any local legislation," Mr North concluded.

Media Contact: Elenore Eriksson,
Director Public Affairs - 02 6246 3716/0419 269 855

[Back to 2005 Media Releases]

GPO Box 1989
Canberra ACT 2601
Australia

Tel: (02) 6246 3788
Fax: (02) 6248 0639
Email: mail@lawcouncil.asn.au

Media Alliance Report on Australian Anti-Terrorism Bill 2005

"It is an impossible position and will lead, needlessly, to demands by the authorities to identify sources and turn over notes and documents received in confidence from their sources.

"If this happens, the ability of journalists to do their jobs evaporates and the ability of the press to fulfil its responsibilities in the public interest disappears."[5]

The Australian Security Intelligence Organisation Act (ASIO Act) also has application to persons not involved in terrorism. However, crucially the ASIO Act incorporates protections that are not mirrored in this Bill.

Further, it is noted that the Joint Standing Committee on ASIO, ASIS and DSD is not due to table its report following its review of the operation and effectiveness and implications of Division 3 Part III of the ASIO Act 1979 until 22 January 2006.[6] Consequently, it is likely to be premature to enact new anti-terror legislation before the assessment of existing powers has been completed.

The Alliance is of the view that consideration of new anti-terror legislation should also await the outcome of the Independent Committee review of the use of the *Security Legislation Amendment (Terrorism) Act 2002*, the *Suppression of Financing of Terrorism Act 2002, the Criminal Code Amendment (Suppression of Terrorist Bombings) Act*, the *Border Security Legislation Amendment Act 2002* and the *Telecommunications Interception Legislation Amendment Act 2002* announced by the Attorney-General on 12 October 2005. That Committee is not due to report until the middle of 2006.[7]

In any event, the provisions of Division 105 of the Bill have the potential to compromise the ability of journalists to work professionally and for the media to work in the public interest.

Power to obtain information and documents and disclosure offences

In Schedule 6 the Bill adds new sections to the *Crimes Act* that cause considerable concern.

Section 3ZQN allows the Australian Federal Police to require a person to produce documents if an officer "considers on reasonable grounds that a person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious terrorism offence".

Section 3ZQO encompasses "the investigation of a serious offence". It is hard to know why, in the context of legislation regarding acts of terrorism, the scope of the Bill has been broadened to capture other offences.

Section 3ZQR does not excuse a person from producing documents under sections 3ZQN or 3ZQO on grounds that to do so "would contravene any other law; or might tend to incriminate the person or otherwise expose the person to a penalty or other liability; or would disclose material that is protected against disclosure by legal professional privilege or any other duty of confidence; or would be otherwise contrary to the public interest."

---

[5] *Publishers lobby for changes to terror law*, Mark Day, The Australian, 10 November 2005, page 17.
[6] The Alliance submission can be found at http://www.aph.gov.au/house/committee/pjcaad/asio_ques_detention/subs/sub65.pdf.
[7] *Independent Committee to Review Security Legislation, Media Release185/2005, The Attorney-General, Philip Ruddock MP, 12 October 2005, available online at http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases_2005_Fourth_Quarter_12_October_2005_-_Independent_committee_to_review_security_legislation_-_1852005*

The Explanatory Memorandum notes: "Care has been taken to ensure sensitive material can not be obtained under the new notice to produce regime. Sensitive material held by health professionals, layers, counsellors and journalists is clearly not caught by the regime. Such sensitive material might be able to be obtained for the purposes of an investigation through a search warrant." It may have been the intention that journalists not be captured in the new notice to produce regime but that intention is not reflected in the Bill itself.

Section 105.41(6) makes it a criminal offence – penalty: imprisonment for five years – to disclose the fact that a preventative detention order has been made in respect of a detainee or disclose any information relayed by that detainee.

The ASIO Act contains secrecy provisions in respect of questioning, production and detention warrants which are also of concern to the Alliance. However, unlike this Bill, the secrecy provisions in the ASIO Act include a provision – section 34VAA(12) – which says: "This section does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication."

This Bill strikes at the basis of news reporting and the principles of freedom of the press. The Alliance can see no demonstrable benefit to be gained by the provisions that will have the effect of stifling freedom of the press and infringing on freedom of political communication.

Appropriately, Section 105.33 of the Bill affords persons detained under the legislation the right "to be treated with humanity and respect for human dignity" and states that such persons "must not be subjected to cruel, inhuman or degrading treatment." Yet, in the event the rights of such a person are violated, the Bill denies the opportunities for such a violation to be reported in the media. Just as astonishing is the fact that the penalty for an officer who commits an offence under this section is two years' imprisonment, compared with the five years' sentence a journalist could face for disclosing the fact of a preventative detention.

The Alliance recommends that, at the very least, section 3ZQR be amended to read as follows:

"3ZQR Documents must be produced

(1) A person is not excused from producing a document under section 3ZQN or 3ZQO on the ground that to do so:
  (a) would contravene any other law; or
  (b) might tend to incriminate the person or otherwise expose the person to a penalty or other liability; or
  (c) would disclose material that is protected against disclosure by legal professional privilege or any other duty of confidence; or
  (d) would be otherwise contrary to the public interest.

(2) However, neither:
  (a) The production of the document; nor
  (b) Any information, document or thing obtained as a direct or indirect consequence of producing the document;

  is admissable in evidence against the person in proceedings other than proceedings for an offence against section 137.1, 137.2 or 149.1 of the *Criminal Code* that relates to this Act.

(3) Despite subsections (1) and (2), a person shall be excused from producing a document under section 3ZQN or 3ZQO on the ground that the production would disclose material that is protected against disclosure by legal professional privilege or any other duty of confidence, including in the case of a journalist, the disclosure of the identity of a confidential source.

(4) A person is not liable to any penalty by reason of his or her producing a document when required to do so under section 3ZQN or 3ZQO."

The Alliance further recommends that, unless otherwise more favourably amended, section 3ZQO be amended by adding a new subsection (5) as follows:

(5) "If the notice specifies that information about the notice must not be disclosed – set out the effect of section 3ZQT (offence for disclosing existence or nature of a notice), provided that any such restriction on disclosure shall not extend beyond 28 days without further order of the Court."

Sedition

The Alliance considers that sedition laws are outdated and unnecessary in the 21st century. Throughout their history they have been used more to curb freedom of speech than to deter acts of terrorism.

That the provisions on sedition contained in Schedule 7 are revisiting arcane laws has been acknowledged by members of the Government. The Attorney-General is sufficiently concerned about the provisions to announce they would be reviewed after the legislation has been enacted and some Government members, including George Brandis MP and Malcolm Turnbull MP, have called for sedition laws to be abolished.

The Alliance agrees with those Government members opposing the sedition provisions and believes the most appropriate course of action would be to delete Schedule 7 in its entirety and to repeal sedition legislation. To review the provisions after they have been legislated rather than before is an odd way to approach a flawed Bill.

The sedition provisions are also unnecessary as all matters contemplated that might be dealt with under the proposed provisions can be dealt with under other legislation, including the *Crimes Act* and anti-vilification legislation.

During the twentieth century, in western developed countries sedition laws fell all but into disuse with some stand-out exceptions – exceptions that demonstrate why sedition laws should be abolished.

The most obvious example is the use of sedition laws to attack the American arts community and Hollywood in particular during McCarthy period in the 1940s and 1950s.

In 1947, the House Committee on Un-American Activites charged ten writers, directors and producers with contempt of Congress for refusing to answer questions posed by the Committee. To become known as the "Hollywood Ten", the most well-known was novelist and screenwriter, Dalton Trumbo. Convicted, he served eleven months in prison and was blacklisted by the industry. Moving to Mexico, he wrote 30 scripts using a pseudonym including the Oscar winning script for *The Brave One* (writing as Robert Rich). It was the use of a pseudonym that enabled *The Bridge Over the River Kwai* to reach the screens. By the end of the notorious McCarthy era somewhere between 325 and 500 actors, directors, producers and writers were forced to seek work elsewhere. For some, it was the end of their career. Some, like Arthur Miller, were able to continue working, Miller writing scripts in New York (where theatre producers ignored the studios' blacklists). Others, like Charlie Chaplin, left the country and never worked in America again. It was not until 1959 that the first crack in the blacklist came with Otto Preminger's decision to hire Dalton Trumbo to write *Exodus*, following which Kirk Douglas announced he would give Trumbo full credit for *Spartacus*. However, as Trumbo himself said, "the blacklist was a time of such evil, no one survived untouched."