THE LEGAL FRAMEWORK IN U.S. LAW FOR SHARING LAW ENFORCEMENT AND INTELLIGENCE INFORMATION

Rebekah Bina
Caroline Nicolai

September 11, 2001 turned our attention to the need for reliable intelligence that could be quickly and effectively shared between government agencies. Information sharing has since become a key policy issue of the current administration. Government studies reveal the urgent need for improvement in order to effectively and precisely combat the dangers of terrorism and ensure the safety of American citizens, both at home and abroad.

This paper provides an overview of the legal authorities governing information sharing, followed by a brief discussion of the recent developments, benefits, and risks in this growing field. The legal framework of information sharing begins with the United States Constitution and continues through statutory enactments and judicial precedent. The authorities include the National Security Act, The Foreign Intelligence Surveillance Act, The Intelligence Authorization Act, and The Homeland Security Act. Notable benefits incurred through information sharing consist of increased ease, accuracy, and thoroughness in identifying and locating terrorists and apprehending suspects. The risks of increased information sharing include possible decreased efficiency as a result of disrupting the traditional culture of the agencies, violation of individual rights, and decreased ability to collect intelligence information. In response to demands for reform the FBI has made recent attempts to improve their information sharing capabilities through personnel reshuffling and task force establishment. The attached chart provides one depiction of the vital players and their interaction within the Intelligence Community.

INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND INTELLIGENCE AGENCIES

The purpose of this paper is to provide background on the status of information sharing between the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI). This paper will briefly discuss the applicable legal framework for information sharing. It will then move into the benefits, risks and barriers to efficient implementation of information between these two agencies. Finally, it will deal with recent developments of the FBI to improve their information sharing capabilities. The attached chart attempts to provide a general map of the structure of the relevant information-sharing and intelligence players.

Legal Authority

Some authority for information sharing can be found in the United States Constitution. Various provisions prescribe the amount and degree of information sharing allowable in order to safeguard separation of powers and individual rights. The Constitution impliedly sets limits on information sharing between the President and Congress, as well as between the people and Congress. Applicable sections dealing with these issues include parts of Articles I and II, and the 1st and 4th Amendments.[1]

Statutes

The National Security Act of 1947 (NSA) was intended to "provide a comprehensive program for the future security of the United States."[2] The Act created the Air Force and reorganized the military branches under the common direction of the Department of Defense and headed by the Secretary of Defense.[3] The NSA also created the National Security Council (NSC) as an auxiliary to the executive branch.[4] Congress stated the function of the National Security Council was to "advise the President with respect to the integration of domestic, foreign and military policies relating to the national security so as to enable the military services and the other departments and agencies of the government to cooperate more effectively in matters involving

national security."[5] Finally, the NSA transformed the Office of Strategic Services into the CIA, vesting it with the nation's intelligence matters related to national security.[6]

The Omnibus Crime Control and Safe Streets Act/1968 Crime Control Act provides the overarching legal framework for law enforcement officials to conduct electronic surveillance and physical searches.[7] In Title III of the act, Congress enumerated conditions for judicial authorization of electronic surveillance.[8] Applications must be approved by the Attorney General before they are presented for a court order.[9]

The Privacy Act of 1974 regulates the federal government's collection, maintenance, use and dissemination of information gathered through surveillance in order to protect the privacy interests of individuals.[10] This act requires that agencies make reasonable efforts to ensure that the information they disseminate is correct and relevant for agency purposes.[11] The Privacy Act requires that an accounting be kept of all disclosed information, including the date, nature of the disclosed information, and recipient of the information.[12] Individuals also have the right to obtain copies of their records held in agency files.[13]

The Foreign Intelligence Surveillance Act of 1978 (FISA) established a legal regime for "foreign intelligence" surveillance.[14] FISA also allows the President to order electronic surveillance for up to one year without a court order in emergency circumstances.[15] This emergency power extends to circumstances where "there is no substantial likelihood" that the communication will involve a U.S. citizen, and the Attorney General meets specific reporting requirements.[16] Under FISA, electronic surveillance is generally allowed with a finding of probable cause that the target if a foreign power or an agent of foreign power, although a criminal action is not required.[17]

The applications for surveillance authorization must identify the federal officer making the application; state the authority under which the application is made; state the identity of the target of surveillance; state the facts concerning justification for the surveillance that the target is a foreign power or agent of foreign power, assert that the pro-

posed surveillance site is used by a foreign power or agent of a foreign power; and provide a description of the methods to be used and a certification that the surveillance would be conducted for an intelligence purpose.[18] The proceedings are non-adversarial and based solely on the Department of Justice's presentations through its Office of Intelligence Policy and Review.[19]

The Freedom of Information Act (FOIA) was enacted upon the premise that "the government and the information of the government belongs to the people."[20] FOIA created a "right to know," allowing any person to access federal agency records, provided that such records are protected under any of nine exemptions.[21] Records held by the FBI pertaining to foreign intelligence, counterintelligence or international terrorism are exempted from disclosure by FOIA.[22] Additionally, records specifically authorized under an Executive Order to be kept secret in the interest of national defense are exempted from disclosure.

The Intelligence Authorization Act of 1997[23] established a division of the National Security Council (NSC), the Committee on Transnational Threats (CTT), to coordinate U.S. efforts in combating terrorist and other organizations.[24] Specifically, this group is tasked to identify transnational threats and develop strategies for responding to their threats. This group also can assist in developing policy and facilitate information sharing between the intelligence community and law enforcement agencies.[25] Additionally, this act allows the intelligence community to collect and share information with law enforcement regarding individuals dwelling outside the United States.[26] Information collected can be used for criminal investigation or prosecution purposes through LEGAT, the FBI agent abroad in charge of international elements of a case involving counterintelligence, criminal investigations, and counterterrorism.

The USA Patriot Act was intended to enhance law enforcement techniques and enhance information sharing between executive agencies.[27] This act removed former barriers to information sharing between law enforcement and intelligence agencies by permitting the disclosure of intelligence information gathered as a result of criminal investigation.[28] This information can be disclosed for the purpose of

aiding a "Federal law enforcement, intelligence, protective, immigration, national defense, or national security official" in his official duties."[29] The USA Patriot Act also amended the Federal Rules of Civil Procedure 6 (e) (3) (C) to allow grand jury information to be disclosed without a court order, "when the material involves foreign intelligence or counterintelligence."[30]

The Homeland Security Act of 2002[31] is an important legal element in the role of sharing information as it established the Department of Homeland Security (DHS) within the Executive Branch. The DHS was developed to aid in the prevention of and "reduce the vulnerability" of the U.S. to acts of terrorism.[32] While the DHS is not tasked with the power to investigate and prosecute acts of terrorism,[33] the act requires the Department to monitor coordination between agencies and subdivisions to ensure that even the most tangential piece of information is analyzed to help secure the homeland.[34] To carry out the demands of the DHS, this act impliedly and expressly demands information sharing between intelligence and law enforcement entities.[35] While the DHS has been given access to information,[36] it is required to share its information, subject to consultation with the CIA.[37] Finally, DHS is required to establish procedures for information sharing to ensure against unauthorized uses and protect individual rights.[38]

The Arming Pilots Against Terrorism Act (APATA) was passed as part of the Homeland Security Act of 2002.[39] It requires TSA to establish the air marshal program and the flight deck officer program to defend aircraft against "acts of criminal violence or air piracy."[40] These programs are a combination of federal government and law enforcement divisions and will require information sharing between intelligence and law enforcement to be effective.

Executive Order 12333 was issued by President Reagan on December 4, 1981 in an effort to better effectuate the conduct of intelligence activities by the United States.[41] This order gave the Director of the Central Intelligence Agency the authority to act as the primary advisor to the President and the National Security Council on foreign intelligence; implement special activities; form policies on foreign intelligence; develop procedures for criminal narcotics intelligence

and facilitate the use of foreign intelligence products by Congress.[42]

The "intelligence community" under this order is limited to "The CIA; NSA; Defense Intelligence Agency; Department of Defense; Bureau of Intelligence and Research of the Department of State; The intelligence elements of the Army, Navy, Air Force and Marine Corps, the FBI, the Department of the Treasury, and the Department of Energy; and the staff elements of the CIA."[43] Under this order the CIA is directed to serve as the primary intelligence service by collecting, coordinating and producing foreign intelligence and counterintelligence to share with the FBI.[44] Therefore, Executive Order 12333 opened the door for information sharing between the FBI and CIA on matters agreed upon by the Director of the CIA and the Attorney General.[45]

Legal Cases

An additional important legal basis for the limitations on information sharing comes from a line of cases establishing judicial precedent regarding information gathering. The following are brief synopses of the most important cases in this area.

In *Katz v. United States* the court considered a fourth amendment claim of invasion of privacy and illegal "search and seizure" as a result of electronically eavesdropping and recording a conversation from a public telephone booth for the purpose of a criminal investigation.[46] The Supreme Court held that the phone booth was not a constitutionally protected area, but that the officers still required a warrant to search regardless of probable cause. The Supreme Court acknowledged that the President had claimed special authority for warrantless surveillance in national security investigations, and explicitly declined to extend its holding to cases "involving the national security."[47]

Unlike *Katz*, in *United States v. United States District Court (Keith)*,[48] the Supreme Court found the authority for national security surveillance implicit in Article II of the Constitution.[49] Justice Powell, on behalf of the court, found that the President's inherent power to protect the national security of the United State is limited by the neutrality of the Constitution on the issue of electronic surveillance.[50] The

court was concerned that privacy rights would be invaded by abuses of power by the Executive Branch.[51] However, Powell found authority for electronic surveillance in the oath clause in Article II.[52] This holding left open the question of whether there exist different warrant standards and procedures in national security investigations than those for normal criminal investigations.[53] The court left open the issue of national security interest abroad concerning surveillance of foreign nations.[54]

A few years later, in *United States v. Truong Dinh Hung*, the Fourth Circuit held that "the Executive Branch need not always obtain a warrant for foreign intelligence surveillance."[55] This might to indicate that the standard for gathering intelligence information on issues of national security is a more relaxed standard that for other criminal issues, allowing for more potentially sharable information.

The Benefits of Information Sharing

Information sharing between intelligence and law enforcement has many benefits, including identifying and locating terrorists easier and faster by enabling informants to piece together necessary information to take effective action. Sharing information allows actions to be taken with more precision and accuracy, as those acting will have a more complete and accurate picture before attempting to locate and apprehend suspects.

In a law review note regarding the threat of transnational organized crime, Pilkerton states "organized crime is a faceless adversary, which, in many circumstances, has the same technical skills, arms capacity and military information that many countries now possess."[56] He notes the importance and need for the law enforcement and the intelligence communities to work together in order to effectively combat this growing economic and physical threat.[57]

Another important benefit of information sharing is that it will help maintain a balance between national security and privacy[58] by preserving the civil liberties of individuals[59] and avoiding problems of racial profiling.[60] Podesta stresses the importance of obtaining quality intelligence information, but notes the need to tread cautiously in

an era where the ease in retrieving information on individuals through cyber monitoring creates issues of invasion of privacy for those conducting legal operations under their 1st and 4th amendment rights.[61] Davis notes that the need for maintaining individual rights in the face of terrorism has resulted in smart legislation that allows for more effective fighting measures.[62]

Additionally, better sharing of information between law enforcement and intelligence can help lead to increased numbers of quality leads and referrals[63] and a reduction in an overlap of jurisdiction.[64] Villaverde implies that if the federal law enforcement were better able to investigate acts of international terrorism because of greater cooperation between intelligence and law enforcement, the government would be better able to pursue more referrals.[65]

Finally, since 9/11 the public has been anxious, wondering how well prepared our country, our cities, and our states are with regard to preventing and responding to attacks. Kellman notes in his article the public concern regarding whether our government is equipped with the tools necessary to identify and assess the threats against the United States and Americans.[66] His article explains the role of various functions of the government and calls for the necessary cooperation with the private sector in order to fully accommodate all needs involved in issues of national threats.[67] Better and increased information sharing can help assure all parties that the government and the states are prepared with adequate information and ability to coordinate and prevent attacks.

The Risks of Information Sharing

However, there are several risks in sharing information between intelligence and law enforcement divisions. In sharing information between these historically separate agencies, the number of people with access to the information naturally increases, decreasing the likelihood that the information will remain classified.[68] This may have a detrimental effect on the ability of CIA agents to collect intelligence as trust may weaken.

The possibility that information may be shared with law enforcement

officials may highly discourage would be informants from relaying their knowledge to intelligence agents. Former Secretary of Defense Frank Carlucci discussed the risk of decreasing sources, noting that this is a real possibility if intelligence assets around the world perceive that the CIA either has no control over the information it is given or will have to disgorge its information upon request.[69]

Additionally, increased sharing may add complexity by blurring the functions of the FBI and CIA.[70] By removing the barriers to information sharing, the specialization of each agency is deteriorated and their roles begin to blur, allowing for increased abuse and dispute of power.[71] The CIA and FBI were purposefully divided and respectively concentrated on intelligence and law enforcement in order to foster competition between the agencies.[72] If information is shared, each agency loses its specialization. Therefore, regulations must be developed that "encourage greater cooperation and coordination of intelligence and law enforcement without giving up the advantages and rivalry."[73]

Finally, the arguably lax rules on information sharing endorsed by the USA Patriot Act may violate the 1st and 4th amendments of the Constitution.[74] The first amendment guarantees citizens that "Congress shall make no law…abridging the freedom of speech" while the fourth amendment guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. As one author, David Hardin, observed:

> The new foreign intelligence purpose standard is absent of the predominance that ensured individual protections were not forsaken at the expense of national security and, thus, antithetical to the protections that the Constitution provides. The result is an open season for law enforcement officials to conduct illegitimate and indiscriminate wiretapping on individuals without the threshold requirements mandated by the Fourth Amendment.[75]

The freedom with which intelligence and law enforcement agencies exchange information as a result of the USA Patriot Act may seriously infringe upon the Constitutional rights of the individual being

investigated. Additionally, there is the difficulty of meeting the separate evidentiary standards that have been developed in law enforcement versus intelligence. Historically, law enforcement procedure requires a substantial basis of evidence in order to charge an individual with a crime. This differs from the intelligence community requirement of probable cause in order to investigate an individual or group of individuals.[76]

These risks bear heavily on the barriers for implementing theories of information sharing.

Recent FBI Developments

In the last year the FBI has made several organizational changes in an effort to improve information sharing.[77] The FBI and the CIA are working together to improve the information regarding national security through direct exchange of both information and personnel.[78] Future plans include sharing office space, video conferencing between agencies, and incorporating representatives from both the FBI and CIA in the Terrorist Threat Integration Center (TTIC).[79] The FBI has also begun corresponding with local law enforcement nationwide through the weekly publication of "Intelligence Bulletins."[80]

An important change has been the reorganization of the Counterterrorism Division. As a result of this reorganization, the FBI and CIA have encountered difficulty in increasing their staff size to meet the growing demand for information sharing.[81] The positions that were created to meet this increased burden resulted in the emergence of the Office of Intelligence as a separate entity.[82] This new department is responsible for monitoring information sharing, managing and promoting the careers of FBI analysts, and managing the FBI's "intelligence units" and "intelligence requirements process."[83] The FBI is also considering developing its own training program for the Office of Intelligence.[84] This program may borrow ideas from the CIA training program for new recruits.[85]

The CTD was reorganized into five sections managed by the Deputy Assistant Director for the Counterterrorism Operations Branch.[86] One of these sections, the Terrorist Financing Operation Section

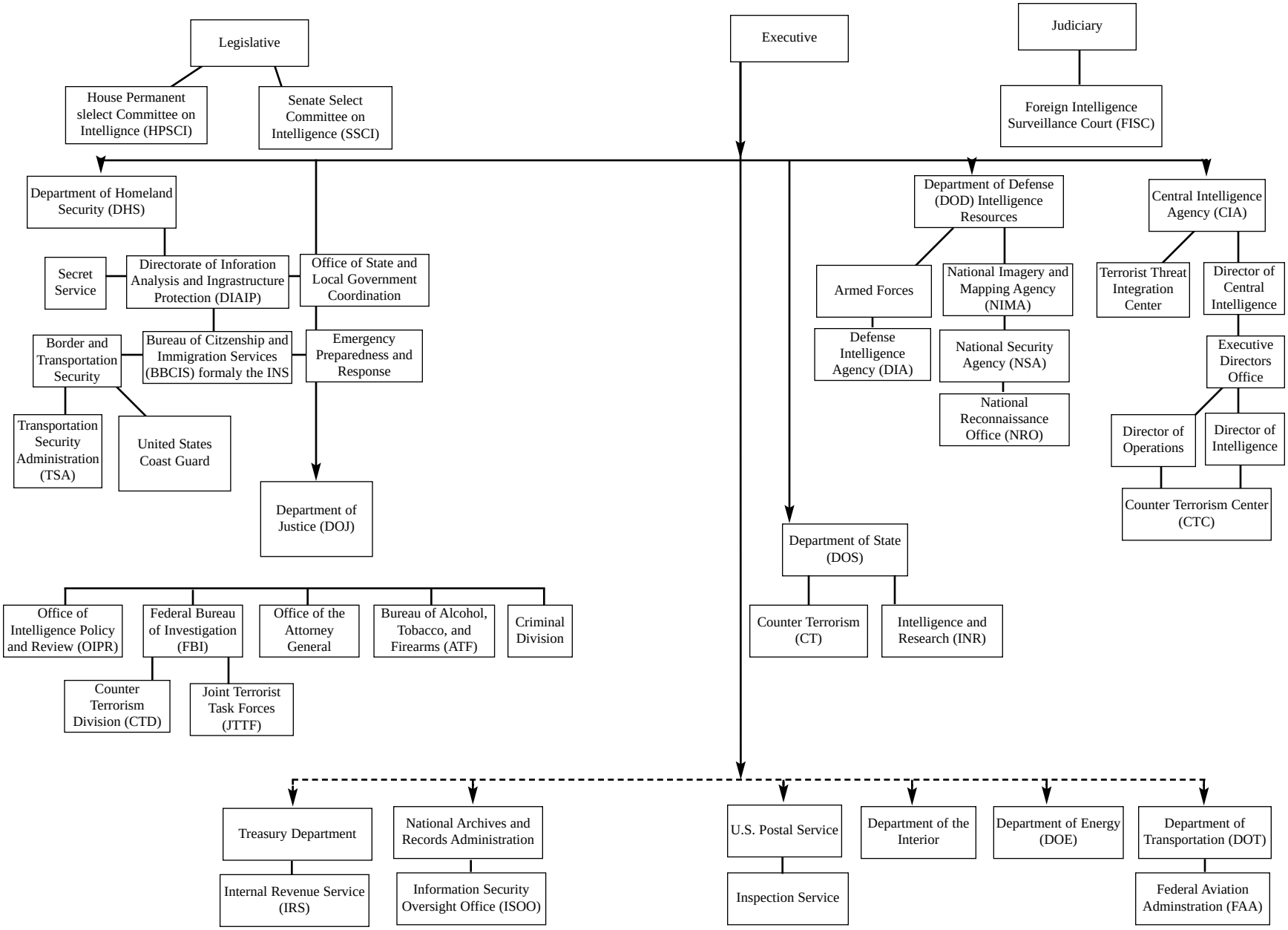
(TFOS), has made advances in improving its information sharing through five initiatives.[87] These initiatives include sharing information with law enforcement communities; identifying patterns of terrorist activities; training Terrorist Financing Coordinators; sharing information with the financial industry; and increasing cooperation with federal, state, and local agencies.[88]

Joint Terrorism Task Forces (JTTF) integrate representatives from federal, state and local law enforcement agencies.[89] The number of JTTFs was increased by the FBI in 2003 to further information sharing capabilities.[90] Three important tasks forces are the Foreign Terrorist Tracking Task Force (FTTTF); The Office of Law Enforcement Coordination (OLEC); and The Terrorist Threat Integration Center (TTIC).[91]

The FTTF was consolidated with the CTD in 2002.[92] The mission of this task force is to control the immigration of aliens with suspected terrorist ties.[93] The OLEC provides guidance to FBI executive and state and local law enforcement regarding information sharing of terrorism information.[94] OLEC's goal is to increase information sharing through technological advances, and delineated responsibilities.[95] The TTIC was developed in 2003 evaluate all intelligence information in order to assess the overall threat to U.S. national security.[96] The purpose of this task force is to provide quick and accurate information that can be shared with federal, state and local law enforcement entities.[97]

In December 2003, the FBI began operating the Terrorist Screening Center (TSC).[98] The TSC is a system that allows patrol officer to run suspects names through a database containing names of known and suspected terrorists.[99] This database is compiled by the National Crime Information Center (NCIC) and still under construction.[100] This program remains controversial as some critics remain concerned on privacy issues.[101]

Despite these developments, there continues to be substantial problems with information sharing. An example is found in the hesitance of the NSA to share information on environmental national security issues.[102] The NSA has continued to refuse to provide regulators with information on contamination.[103]


Legislative
House Permanent slelect Committee on Intellignce (HPSCI)
Senate Select Committee on Intelligence (SSCI)
Executive
Judiciary
Foreign Intelligence Surveillance Court (FISC)
Department of Homeland Security (DHS)
Secret Service
Directorate of Inforation Analysis and Ingrastructure Protection (DIAIP)
Office of State and Local Government Coordination
Border and Transportation Security
Bureau of Citzenship and Immigration Services (BBCIS) formaly the INS
Emergency Preparedness and Response
Transportation Security Administration (TSA)
United States Coast Guard
Department of Justice (DOJ)
Department of Defense (DOD) Intelligence Resources
Armed Forces
National Imagery and Mapping Agency (NIMA)
Defense Intelligence Agency (DIA)
National Security Agency (NSA)
National Reconnaissance Office (NRO)
Central Intelligence Agency (CIA)
Terrorist Threat Integration Center
Director of Central Intelligence
Executive Directors Office
Director of Operations
Director of Intelligence
Counter Terrorism Center (CTC)
Department of State (DOS)
Counter Terrorism (CT)
Intelligence and Research (INR)
Office of Intelligence Policy and Review (OIPR)
Federal Bureau of Investigation (FBI)
Office of the Attorney General
Bureau of Alcohol, Tobacco, and Firearms (ATF)
Criminal Division
Counter Terrorism Division (CTD)
Joint Terrorist Task Forces (JTTF)
Treasury Department
Internal Revenue Service (IRS)
National Archives and Records Administration
Information Security Oversight Office (ISOO)
U.S. Postal Service
Inspection Service
Department of the Interior
Department of Energy (DOE)
Department of Transportation (DOT)
Federal Aviation Adminstration (FAA)

ENDNOTES

[1] William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance* 50 Am. U. L. Rev. 1, 48, 51 (2000).

[2] 50 U.S.C. §401.

[3] 50 U.S.C. §410(b).

[4] 50 U.S.C. §402.

[5] 50 U.S.C. §402(a).

[6] 50 U.S.C. §403(a).

[7] 18 USCA § 2510 (1968)

[8] Banks & Bowman, *supra* note 1.

[9] Id. at § 2510(1),(7)

[10] Steven Dycus et. al, National Security Law, 953 (2002).

[11] 5 U.S.C. §552(A)(d)(6).

[12] Id. at (c)(1).

[13] Id. at (d)(2).

[14] Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811, 1821-1829, 1841-1846, 1861-62).

15 Banks & Bowman, supra note 1, at 89.

[16] *Id. citing* 50 U.S.C. §1802(a)(1).

[17] Pub. L. No. 95-511.

[18] 50 U.S.C. §1804(a).

[19] Id.

[20] Dycus, *supra* note 10, at 923.

21 Id. at 924; 5 U.S.C. §552(b).

[22] 5 U.S.C. §552(c)(3).

[23] 50 U.S.C. § 403 (1997)

[24] Id. at § 402(h)(2)

[25] Id. at § 402(i)(3-4)

[26] Id. at § 403-5(a)

[27] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, PL 107-56, October 26, 2001.

[28] Id. at §203(d)(1); See also Michael T. McCarthy, *Recent Development: USA Patriot Act*, 39 Harv. J. on Legis. 435, (Summer, 2002).

[29] Id.

[30] Id. at §203(a)(1); See also Gregory F. Treverton, *Terrorism, Intelligence and Law Enforcement: Learning the Right Lesson*, June 3, 2003 at 14.

[31] PL 107-296, 2002 HR 5005.

[32] Id. at § 101(b)(1).

[33] Id. at § 101(b)(2)

[34] Id. at § 101(b)(1)

[35] Id. at § 102(c)(d)(f), see generally § 202

[36] Id. at §§ 202, 212(5)

[37] Id. at §§ 202(c)(2), 214

[38] Id. at §221

[39] See 6 U.S.C.A. § 513, 49 U.S.C.A. § 44921 (enacted); 49 U.S.C.A. §§ 44903, 44918 (amended); 49 U.S.C.A. §§ 114, 44903 (repealed). See generally 49 U.S.C Chapters 1-7 (This document contains the portion of Title 49 of the U.S. Code concerning the organization general duties and powers of the Department of Transportation) and 49 U.S.C. Chapters 401-501 (This document contains the portion of Title 49 of the U.S. Code concerning aviation programs)

[40] See 6 U.S.C.A. § 513; 49 U.S.C.A. § 44921

[41] 46 Fed. Reg. 59,941 (1981), preamble.

[42] Id. at §1.4.

[43] 46 Fed. Reg. 59,941 (1981), at §3.4(f).

[44] Id. at §1.8.

[45] Id.

[46] 389 U.S. 347 (1967).

[47] Id. at 358, FN 23

[48] 407 U.S. 297 (1972).

[49] William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror* 10 (37 U. Miami Law Review 2003).

[50] Banks & Bowman, supra note 1, at 50-51.

[51] Id.

[52] Id.

[53] Banks, supra note 49, at 12.

[54] Banks & Bowman, supra note 1, at 52.

[55] 629 F.2d 908, 913 (4th Cir. 1980)

[56] Id. at 247-48.

[57] Christopher M. Pilkerton, *Changing The Chameleon: A New Approach To The Investigation Of Transnational Organized Crime*, 10 Int'l Legal Persp. 247,277-78 (1998)

[58] See generally Lance Davis, *The Foreign Intelligence Surveillance Court's May 17 Opinion: Maintaining A Reasonable Balance Between National Security And Privacy Interests*, 34 McGeorge L. Rev. 713 (2003)

[59] See generally John Podesta, *USA PATRIOT ACT The Good, the Bad, and the Sunset*, 29-WTR Hum. Rts. 3 (2002)

[60] See generally Deborah A. Ramirez, Jennifer Hoopes, Tara Lai Quinlan, *Defining Racial Profiling In A Post-September 11 World*, 40 Am. Crim. L. Rev. 1195 (2003) (noting the problems since 9/11 with racial profiling). See also H. Peter Del Bianco, Jr. And F. Mark Terison, *Is Big Brother Watching Out For Us?*, 17 MEBJ 20 (2002) (noting issues of privacy).

[61] See generally Podesta, supra note 59.

[62] See supra note 59 at 724. See also H. Peter Del Bianco, Jr. And F. Mark Terison, *Is Big Brother Watching Out For Us?*, 17 MEBJ 20 (2002) (noting the recent acts as a balancing of privacy and national security issues).

[63] See generally Mark D. Villaverde, *Structuring The Prosecutor's Duty To Search The Intelligence Community For Brady Material*, 88 Cornell L. Rev. 1471, 1474 (2003)

[64] See generally Jonathan M. Fredman, *Intelligence Agencies, Law Enforcement, And The Prosecution Team*, 16 Yale L. & Pol'y Rev. 331 (1998).

[65] See supra note 63, at 1474.

[66] See generally Barry Kellman, *Catastrophic Terrorism—Thinking Fearfully, Acting Legally*, 20 Mich. J. Int'l L. 537 (1999).

[67] Id.

[68] See generally Mary MS Wong, *Electronic Surveillance and Privacy in the United States After September 11, 2001: The USA Patriot Act*, 2002 Sing. J. Legal Stud. 214 (2002).

[69] William S. Cohen, *Congressional Oversight of Covert Actions: The Public's Stake in the Forty-Eight Hour Rule*, 12 Harv.J.L.& Pub. Pol'y 285, (1989) at FN 39, citing *Proposed Oversight Legislation: Hearings Before Senate Select Comm. On Intelligence*, 100th Cong. 203-206 (1988) (statement of Secretary of Defense Frank Carlucci).

[70] Jennifer C. Evans, Hijacking Civil Liberties: The USA Patriot ACT of 2001, 33 Loy. U. Chi. L. J. 933 (Summer, 2002) at FN 340.

[71] Id.

[72] Banks, supra note 49 at 6-8.

[73] Id. at 6.

[74] See generally Heath H. Galloway, *Don't Forget What We are Fighting For: Will the Fourth Amendment Be a Casualty of the War on Terror*? 59 Wash. & Lee L. Rev. 921 (Summer, 2002); Steven W. Becker, *Mirror, Mirror on the Wall...Assessing the Aftermath of September 11th*, 37 Val. U. L. Rev. 563, (Spring, 2003); John W. Whitehead, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives*, 51 Am. L. Rev. 1081, (2002); Peter P. Swire, *Security and Privacy after September 11: The Health Care Example*, 71 Geo. Wash. L. Rev. 291, (2002).

[75] David Hardin, *The Fuss Over Two Small Words: The Unconstitutionality of the USA Patriot Act Amendments to FIA Under the Fourth Amendment*, 71 Geo. Wash. L. Rev. 291, 345 (2003).

[76] See generally Treverton, supra note 30.

[77] U.S. Dep't of Justice, Office of the Inspector General Audit Division *The Federal Bureau of Investigations Effort to Improve the Sharing of Intelligence and Other Information*, Audit Report 04-10, 28 (Dec. 2003).

[78] Id.

[79] Id. at 28-29.

[80] Id. at 58-60.

[81] Audit Report, supra 77, at 30-32.

[82] Id. at 31.

[83] Id. at 32.

[84] Id.

[85] Id.

[86] Id. at 33.

[87] Id.

[88] Id.

[89] Id. at 41

[90] Id.

[91] Id. at 42-46.

[92] Id. at 43.

[93] Id.

[94] Id. at 44.

[95] Id.

[96] Id. at 44-45.

[97] Id. at 45.

[98] *Secrecy News*, FAS Project on Government Secrecy, "FBI Opens Terrorist Screening Center" December 4, 2003. available at http://www.fas.org/irp/agency/doj/fbi/fbi-tsc.pdf.

[99] Id.

[100] Id.

[101] Id.

[102] Rona Kobell & Ariel Sabar, "NSA says its toxic waste is classified" *Balt. Sun* Dec. 30, 2003. available at http://tinyurl.com/2xxnn.

[103] Id.

Law Enforcement Access to Data. Because the amount of data continues to grow and our laws have not been updated to keep pace with the change in the technology landscape, during the past few years we have seen various legal challenges between technology companies and the U.S. government pertaining to law enforcement access to data. Such challenges will likely become more common with the rise of AI systems.Â Dennis is a Fellow of Information Privacy, a Certified Information Privacy Professional/United States and a Certified Information Privacy Technologist with the International Association of Privacy Professionals. He serves on the Board of Directors of Illinois Legal Aid Online and the Association of Corporate Counsel â€“ Chicago Chapter. Law Enforcement. Criminal intelligence and information sharing I Countering kidnapping I Border management I Container Control. In every country in the world, law enforcement officials are at the frontline of efforts to combat organized crime. The building of criminal investigative and other law enforcement capacity is a core component of UNODC's work.Â UNODC delivers a range of trainings to law enforcement officers on topics of relevance to fighting organized crime in their local contexts. It also employs modern technical training such as computer-based training as well as assistance in improving information exchange between law enforcement agencies, custom and border control authorities in different countries. The information activities of law enforcement can be broken into three categories. Gathering and analyzing information to determine that a law has been violated; Gathering and analyzing information to determine the identity of the person or persons responsible for a violation of law; and.Â None of these concerns about balancing the need for law enforcement agencies to gather information and the need of the citizen for privacy are new. What is new are the modern information technologies that law enforcement agencies can now use to observe situations and identify individuals more quickly, more accurately, and at less expense than ever before. o Collection of intelligence operates from US area o Federal, state, and local law enforcement o Shares info from all sources. Critique of intelligence gathering. â€¢ Intelligence is just a means, not an end â€¢ Suspending civil rights has downsides â€¢ Problem of intelligence self-interest â€¢ Need cooperation and information sharing to make it work â€¢ Need realistic expectations: intelligence is guesswork o The goal is safety and security, not intelligence gathering. How terrorism ends.Â military vs. law enforcement. In some countries, military performs ordinary police functions but others restrict military control in enforcing domestic population (other than anarchy and insurrection). National police vs. decentralized police. Security and intelligence services: legal framework. France Country Report Germany Country Report Italy Country Report Netherlands Country Report. 3.Â Table 3: Specific legal provisions for law enforcement hacking in four Member States. 42.Â Hacking by law enforcement is a relatively new phenomenon within the framework of the longstanding public policy problem of balancing security and privacy. On the one hand, law enforcement agencies assert that the use of hacking techniques brings security, stating that it represents a part of the solution to the law enforcement challenge of encryption and â€˜Going Darkâ€™ without systematically weakening encryption through the introduction of â€˜backdoorsâ€™ or similar techniques.