Order Code RL31730

Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws

Updated March 21, 2003

Gina Marie Stevens
Legislative Attorney
American Law Division

The author wishes to thank Attorneys Maureen Murphy and Charles Doyle of the American Law Division for their substantial contributions to this report.

Privacy: Total Information Awareness Programs and Related Information Access, Collection and Protection Laws

Summary

This report describes the Total Information Awareness (TIA) programs in the Defense Research Projects Agency (DARPA) of the Department of Defense, and related information access, collection, and protection laws. TIA is a new technology under development that plans to use data mining technologies to sift through personal transactions in electronic data to find patterns and associations connected to terrorist threats and activities. Data mining technologies are currently used by federal agencies for various purposes. DARPA has underway a five year research project to develop and integrate information technologies into prototype systems to identify foreign terrorists for use by the intelligence, counterintelligence, law enforcement, and homeland security communities. Recent increased awareness about the existence of the TIA project provoked expressions of concern about the potential for the invasion of privacy of law-abiding citizens by the Government, and about the direction of the project by John Poindexter, a central figure in the Iran-Contra affair. While the law enforcement and intelligence communities argue that more sophisticated information gathering techniques are essential to combat today's sophisticated terrorists, civil libertarians worry that the Government's increased capability to assemble information will result in increased and unchecked government power, and the erosion of individual privacy. A coalition of public interest groups has asked Congress to intervene.

Significant policy and legal issues are raised by the government's TIA plans. Chief among them are privacy issues involving questions of access to, and use and disclosure of personal information by the federal government. This report describes current laws and safeguards to protect the privacy of personal information, the required legal process for officials who seek access to information, and the provisions currently in place that permit access and dissemination of information for law enforcement, intelligence, and terrorism purposes. Federal laws currently protect government, credit, communications, education, bank, cable, video, motor vehicle, health, telecommunications, children's, and financial information; generally carve out exceptions for disclosure of personal information; and authorize use of warrants, subpoenas, and court orders to obtain information.

Some Members of Congress seek additional Congressional oversight of TIA programs. Legislation has been introduced in the 108th Congress regulating TIA programs. On January 23, 2003, the Senate passed amendment S.Amdt. 59 to H.J.Res. 2, the Omnibus Appropriations Act for Fiscal Year 2003, imposing limitations on the unfolding Total Information Awareness programs, and requiring a detailed report to Congress. On February 13, 2003, both the House and Senate approved the Fiscal Year 2003 omnibus spending bill (P.L. 108-7) including, with slight modifications, the language from S.Amdt. 59. For more information, see CRS Report RL31786, Total Information Awareness Programs: Funding, Oversight and Composition Issues by Amy Belasco; and CRS Report RL31798, *Data Mining: An Overview,* by Jeffrey Seifert. This report will be updated as warranted.

Contents

List of Tables

Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws

Total Information Awareness Programs

The September 11th terrorist attacks increased government awareness of the inadequacies of its information gathering techniques, its information technology, and its information holdings. To remedy this situation various federal agencies are addressing issues that may possibly have a direct bearing on the balance between the government's need for information and an individual's expectation of privacy in their information. This report describes the Total Information Awareness (TIA) programs underway in the Department of Defense (DOD) which may develop prototype research and development technologies for information gathering and analysis capabilities that could be used by DOD and other agencies. It will then discuss current laws and safeguards to protect the privacy of personal information, the provisions currently in place that permit access and dissemination of information for law enforcement, intelligence, and terrorism purposes, and the required legal process for officials who seek access to information.

The TIA program is being developed by the Defense Advanced Research Projects Agency (DARPA) of the Department of Defense in the Information Awareness Office (IAO)[1] as an experimental prototype system that integrates three types of technologies — machine translation of languages; data search and pattern recognition; and advanced collaborative and decision support.[2] DARPA "aspires to create the tools that would permit analysts to data-mine an indefinitely expandable universe of databases" "to analyze, detect, classify and identify foreign terrorists – and decipher their plans – and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts."[3] The TIA system is designed to be a tool in the war against terrorism that "would, among other things, help analysts

---

[1] The Total Information Awareness program will integrate some or all of the R&D efforts that are managed by the Information Awareness Office, including Project Genoa, Project Genoa II, Genisys, Evidence Extraction and Link Discovery, Wargaming the Asymmetric Environment, Translingual Information Detection, Extraction and Summarization, Human Identification at a Distance, Bio-Surveillance, Communicator, and Babylon, as well as possibly other R&D developed by DARPA, DOD, other federal agencies, and the private sector. See CRS Report RL31786, *Total Information Awareness Programs: Funding, Oversight and Composition Issues,* by Amy Belasco.

[2] See Defense Advanced Research Projects Agency's Information Awareness Office and Total Information Awareness Project at [http://www.darpa.mil/iao/programs.htm].

[3] [http://www.darpa.mil/iao/TIASystems.htm].

search randomly for indications of travel to risky areas, suspicious emails, odd fund transfers and improbable medical activity, such as the treatments of anthrax sores."[4] The goal of the TIA program is "to create a counter-terrorism information system that: (i) increases the information coverage . . . ; (ii) provides focused warnings within an hour after a triggering event occurs or an evidence threshold is passed; [and] (iii) can automatically cue analysts based on partial pattern matches and analytical reasoning, and information sharing . . . ."[5] DARPA's five year research project to develop and integrate information technologies into a prototype system for use by the intelligence, counterintelligence and law enforcement communities intends to exploit R&D efforts that have been underway for several years in DARPA and elsewhere, as well as private sector data mining technology.[6]

DARPA envisions a database "of an unprecedented scale, [that] will most likely be distributed, must be capable of being continuously updated, and must support both autonomous and semi-automated analysis."[7] Extensive existing databases from both private and public sector information holdings will be used to obtain transactional and biometric data.[8] Transactional data for the TIA database could include financial (*e.g.*, banks, credit cards, and money transmitters, casinos and brokerage firms), educational, travel (*e.g.*, airlines, rail, rental car), medical, veterinary, country entry, place/event entry, transportation, housing, critical resources, government, and communications (*e.g.*, cell, landline, Internet) data. Biometric data for the database could include face, finger prints, gait, and iris data.[9] The TIA system could seek access to databases to discover connections between "passports; visas; work permits; driver's license; credit card; airline tickets; rental cars; gun purchases; chemical purchases – and events – such as arrest or suspicious activities and so forth."[10]

Data Mining

A key component of the TIA program is the deployment of data mining technologies to sift through data and transactions to find patterns and associations to discover and track terrorists.[11] The idea is that "if terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions and they will leave signatures in this information space. . . ."[12] TIA

---

[4] Robert O'Harrow, *U.S. Hopes to Check Computers Globally; System Would Be Used to Hunt Terrorists*, Washington Post A4 (Nov. 12, 2002).

[5] [http://www.darpa.mil/body/NewsItems/pdf/DARPAfactfile.pdf].

[6] [http://www.darpa.mil/iao/BAA02-08.pdf].

[7] [http://www.darpa.mil/iao/TIASystems.htm].

[8] [http://www.darpa.mil/iao/solicitations.htm].

[9] See John Woodward, Jr., Rand Corporation, Superbowl Surveillance: Facing Up to Biometrics (2001) available at [http://www.rand.org/publications/IP/IP209/IP209.pdf].

[10] Solicitations, supra note 8.

[11] See CRS Report RL31798, *Data Mining: An Overview*, by Jeffrey Seifert.

[12] [http://www.darpa.mil/DARPATech2002/presentations/iao_pdf/speeches/POINDEXT.

plans to mine transaction data for terrorism-related indicators to uncover terrorists plans or attacks. Data mining is the search for significant patterns and trends in large databases using sophisticated statistical techniques and software.[13] The widespread use of computers, and the large amount of information maintained in databases means that there exists a vast repository of information useful for antiterrorism purposes. Today, "it is a rare person in the modern world who can avoid being listed in numerous databases."[14] Data mining technologies facilitate the use of information.

Data mining technologies are currently used by federal agencies for various purposes, and plans exist for considerable expansion of this technology. For example, the Department of Justice is engaged in data mining projects that utilize computer technology to analyze information to reveal patterns of behavior consistent with terrorist activities. Utilizing law enforcement and intelligence information as well as public source data, the Foreign Terrorist Tracking Task Force employs risk modeling algorithms, link analysis, historic review of past patterns of behavior, and other factors to distinguish persons who may pose a risk of terrorism from those who do not.[15] The Transportation Security Administration's Computer- Assisted Passenger Profiling System is widely employed by the airlines.[16] The National Strategy for Homeland Security includes several initiatives to integrate terrorist-related information from the databases of all government agencies responsible for homeland security. Under this initiative, the Department of Homeland Security, Department of Justice, FBI, and numerous state and local law enforcement agencies would have access to information analysis, using advanced data-mining techniques to reveal patterns of criminal behavior and detain suspected terrorists before they act.[17] Additionally, on January 28, 2003 President Bush proposed to establish a new Terrorism Threat and Integration Center to merge and analyze terrorist-related information collected domestically and abroad.[18]

DOD recently announced plans to form an internal TIA oversight board to establish policies and procedures for use of TIA within and outside of DoD, and to

---

[12] (...continued)
pdf].

[13] Carol Pickering, *They're Watching You: Data-Mining Firms Are Watching Your Every Move – and Predicting the Next One*, Business 2.0 (Feb. 2000) at [http://www.business2.com].

[14] Whitfield Diffie and Susan Landau Diffie, Privacy on the line: the Politics of Wiretapping and Encryption at119 (1998).

[15] The White House Office of Homeland Security, The National Strategy for Homeland Security at 39 (July 2002) at [http://www.whitehouse.gov/homeland/book/index.html].

[16] Section 307 of the Federal Aviation Reauthorization Act of 1996 (P.L. 104-264, 110 Stat. 3253) directed FAA to assist airlines in developing a computer-assisted passenger profiling system in conjunction with other security measures and technologies. See [http://www.house.gov/transportation/aviation/02-27-02/02-27-02memo.html].

[17] Supra note 14.

[18] [http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html].

establish an external federal advisory committee to advise the secretary of Defense on policy and legal issues raised by TIA technologies.[19]

Legal Issues

Government access to and mining of information on individuals held in a multiplicity of databases, public and private, raises a plethora of issues – both legal and policy. To what extent should the government be able to gather and mine information about individuals to aid the war against terrorism?[20] Should unrestricted access to personal information be permitted? Should limitations, if any, be imposed on the government's access to information? In resolving these issues, the current state of the law in this area may be consulted. The rest of this report describes current laws and safeguards to protect the privacy of personal information, the required legal process for officials who seek access to information, and the provisions currently in place that permit access and dissemination of information for law enforcement and intelligence gathering purposes. Following is a description of selected information access, collection, and disclosure laws and regulations.

Federal Laws Governing Federal Government Access to Information

Generally there are no blanket prohibitions on federal government access to publicly available information (*e.g.*, real property records, liens, mortgages, etc.). Occasionally a statute will specifically authorize access to such data. The USA PATRIOT Act, for example, in transforming the Treasury Department's Financial Crimes Enforcement Network (FinCEN) from an administratively established bureau to one established by statute, specified that it was to provide government-wide access to information collected under the anti-money laundering laws, records maintained by other government offices, as well as privately and publicly held information. Other government agencies have also availed themselves of computer software products that provide access to a range of personal information. The FBI reportedly purchases personal information from ChoicePoint Inc, a provider of identification and credential verification services, for data analysis.[21]

---

[19] Available at [http://www.defenselink.mil/news/Feb2003/t02072003_t0207atl.html].

[20] The Markle Foundation Task Force on National Security in the Information Age recently proposed guidelines to allow the effective use of information (including the use of data mining technologies) in the war against terrorism while respecting individuals' interests in the use of private information. The Markle Foundation Task Force on National Security in the Information, Protecting America's Freedom in the Information Age at 32 - 34 (October 2002) at [http://www.markle.org/news/NSTF_Part_1.pdf].

[21] Glenn R. Simpson, "*Big Brother-in-Law: If the FBI Hopes to Get The Goods on You, It May Ask ChoicePoint — U.S. Agencies' Growing Use Of Outside Data Suppliers Raises Privacy Concerns*" Wall Street Journal, April 13, 2001 (The company "specialize[s] in doing what the law discourages the government from doing on its own– culling, sorting and packaging data on individuals from scores of sources, including credit bureaus, marketers and regulatory agencies.")

As previously discussed the federal government seeks access to publicly and privately held databases in order to build a centralized database to detect and deter against terrorist threats and attacks. This section of the report describes existing legal safeguards for the protection of personal information. It covers applicable federal laws; a discussion of state laws is beyond its scope. In the United States there is no omnibus statute or constitutional provision that provides comprehensive legal protection for the privacy of personal information, but rather an assortment of laws regulate information deemed to be of sufficient importance to be afforded some level of protection. The U.S. Constitution, federal statutes and regulations, and state law combine to govern the collection, use, and disclosure of information. The Constitution provides certain privacy protections, but does not explicitly protect information privacy.[22] Its protections extend only to the protection of the individual against government intrusions, and its guarantees are not applicable unless "state action" has taken place. In other words its guarantees extend to government intrusions rather than private sector abuses. The Fourth Amendment search-and-seizure provision protects a right of privacy by requiring warrants before government may invade one's internal space or by requiring that warrantless invasions be reasonable.[23] That amendment protects individual privacy against certain kinds of governmental intrusion. The Supreme Court has interpreted this language as imposing a warrant requirement on all searches and seizures predicated upon governmental authority, and has ruled that violations of this standard will result in the suppression in any criminal proceeding of any material or information derived therefrom. The Court has also recognized exceptions to the warrant requirement. Finally, an individual has no Fourth Amendment rights with respect to information held by third parties.[24]

There is no comprehensive federal statute that protects the privacy of personal information held by the public sector and the private sector. Instead federal law tends to employ a sectoral approach to the regulation of personal information. Historically, the individual's privacy interests have been balanced with the government's information needs.[25] Examples of this balancing of personal and governmental interests can be found in the numerous privacy-related enactments of the past twenty-five years. Federal laws protect government, credit, communications, education, bank, cable, video, motor vehicle, health, telecommunications, children's, and financial information. These laws generally carve out exceptions for the disclosure of personally identifiable information to law enforcement officials, and authorize access to personal information through use of search warrants, subpoenas, and court orders. Notice requirements vary according to statute.

---

[22] *Whalen v. Roe*, 429 U.S. 589 (1977).

[23] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV.

[24] *United States v. Miller*, 425 U.S. 435 (1976).

[25] Privacy Protection Study Commission, Personal Privacy in an Information Society (1977).

Federal Government Information.

The Privacy Act. The Privacy Act of 1974, 5 U.S.C. § 552a, was implemented to protect the privacy of individuals identified in information systems maintained by federal executive branch agencies, and to control the collection, use, and sharing of information. The Act restricts disclosure of personally identifiable records maintained by agencies; grants individuals increased rights of access to agency records maintained on themselves; grants individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete; and establishes a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

The general exemptions of the Privacy Act, which are agency and function-oriented, permit the Central Intelligence Agency[26] and federal criminal law enforcement agencies to exempt certain systems of records from some of the Act's requirements.[27] The general exemption for the CIA covers all of its files. The general exemption for federal criminal law enforcement agencies covers identification information, criminal investigative materials, and reports compiled between the stages of arrest and release from criminal agency supervision. An agency which has law enforcement, prosecution, or probation activities can use this general exemption. In addition specific exemptions permit an agency to exempt a system of records from specified Privacy Act requirements if the system of records is: national security information which would be protected from mandatory disclosure by FOIA;[28] law enforcement material which falls outside the criminal law enforcement general exemption; Secret Service files; Census material and other matter required by law to be kept only as a statistical record; confidential sources of government background investigation information; test materials of the civil service selection and promotion process; and confidential evaluations of military and naval personnel.[29]

The general disclosure rule under the Privacy Act is that unless a statutory exception applies, no federal executive branch agency shall disclose any record which is contained in a system of records to *any person* or to *another agency* except pursuant to a written request by, or with prior written consent of the individual to whom the record pertains.[30] Disclosure includes dissemination within the executive branch from one agency to another or from one large segment of an agency to another segment.[31] This rule would appear to prohibit the sharing of personal information

---

[26] 32 CFR Part 109.

[27] 5 U.S.C. § 552a(j).

[28] 5 U.S.C. § 552(b)(1). Exemption 1 of the FOIA protects from disclosure national security information concerning the national defense or foreign policy, provided that it has been properly classified in accordance with the requirements of an executive order.

[29] 5 U.S.C. § 552a(k).

[30] 5 U.S.C. § 552a(b).

[31] Office of Management and Budget, Guidelines for Implementing Section 552a of Title 5, (continued...)

collected by one agency with other agencies for purposes other than for which it was originally collected. In reality, though, the Act's many exemptions and exceptions ease this prohibition. Many of the exceptions – as well as specific laws authorizing sharing of records – permit an agency to disclose or share personal information with other agencies.[32]

Several of the statutory exemptions are relevant to the information collection and sharing activities of the Total Information Awareness system, and would appear to authorize the disclosure of personal information in federal records systems without the individual's consent.[33] The routine use exemption allows an agency to share, without consent, an individual's personal information with other agencies if that sharing is listed as a routine use for that agency in the Federal Register and is compatible with the purpose of the initial information gathering.[34] The January 2003 publication by the Transportation Security Administration of a notice to amend the "Aviation Security Screening Records" system of records illustrates how broadly records can be disclosed pursuant to the routine use exemption, without the consent of the subject of the record, for agency purposes.[35] The exemption for civil and

---

[31] (...continued)
at 6 (1975).

[32] 5 U.S.C. § 552a(b).

[33] See Sean Fogarty and Daniel R. Ortiz, "Limitations Upon Interagency Information Sharing: The Privacy Act of 1974" in The Markle Foundation Task Force Report, National Security in the Information Age at 127 - 132 (October 2002).

[34] 5 U.S.C. § 552a(b)(3). The OMB guidelines state that the "compatibility" concept encompasses functionality equivalent uses, and other uses that are necessary and proper.

[35] Records in the system include passenger name records (PNRs) and associated data; reservation and manifest information of passenger carriers and, in the case of individuals who are deemed to pose a possible risk to transportation security, record categories may include: risk assessment reports; financial and transactional data; public source information; proprietary data; and information from law enforcement and intelligence sources. Data are retrievable by the name or other identifying information of the individual, such as flight information. Information may be disclosed from this system as follows (routine uses of records): (1) to appropriate Federal, State, territorial, tribal, local, international, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, ... (2) to contractors, grantees, experts, consultants, agents and other non-Federal employees performing or working on a contract, service, grant, cooperative agreement, or other assignment from the Federal government for the purpose of providing consulting, data processing, clerical, or other functions to assist TSA . . . . (3) to Federal, State, territorial, tribal, and local law enforcement and regulatory agencies–foreign, international, and domestic–in response to queries regarding persons who may pose a risk to transportation or national security; a risk of air piracy or terrorism or a threat to airline or passenger safety; or a threat to aviation safety, civil aviation, or national security. (4) to individuals and organizations, in the course of enforcement efforts, to the extent necessary to elicit information pertinent to the investigation, prosecution, or enforcement of civil or criminal statutes, rules, regulations or orders regarding persons who may pose a risk to transportation or national security; a risk of air piracy or terrorism or a threat to airline or passenger safety; or a threat to aviation safety, civil aviation, or national security. (5) to a Federal, State, or local agency, where such
(continued...)

criminal law enforcement activities permits the disclosure of personal information for legally authorized activities.[36] This exemption would allow the disclosure of information to an intelligence agency for the prevention of terrorist acts. The exemption for foreign counterintelligence in the Computer Matching and Privacy Protection Act of 1988,[37] which amended the Privacy Act, legitimizes information sharing through data matching among agencies for national security purposes.[38]

Agencies are required to make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.

Education Information.

The Family Educational Rights and Privacy Act of 1974. FERPA governs access to and disclosure of personally identifiable information in educational records held by federally funded educational institutions and agencies.[39] Disclosure requires prior consent of the student's parents unless done pursuant to federal grand jury subpoena, administrative subpoena, or court order for law enforcement purposes. Upon good cause shown, the court shall order that the existence or contents of a subpoena or the information furnished not be disclosed. The USA PATRIOT Act of 2001 amended FERPA to authorize the Justice Department to obtain a court order to collect education records relevant to a terrorism-related offense or an act of domestic or international terrorism.[40] The order can only be issued if a court finds that the records are relevant to a terrorism investigation. The amendment also protects educational institutions from liability for complying with such order.

---

[35] (...continued)
agency has requested information relevant or necessary for the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit. (6) to the news media . . . . (7) to the Department of State, or other Federal agencies concerned with visas and immigration, and to agencies in the Intelligence Community, to further those agencies' efforts with respect to persons who may pose a risk to transportation or national security; a risk of air piracy or terrorism or a threat to airline or passenger safety; or a threat to aviation safety, civil aviation, or national security. (8) to international and foreign governmental authorities in accordance with law and . . international agreements. (9) in proceedings before any court, administrative, adjudicative, or tribunal body before which TSA appears, . . . provided, however, that in each case, TSA determines that disclosure of the records in the proceeding is a use of the information contained in the records that is compatible with the purpose for which the records were collected. (10) to airports and aircraft operators . . .. (11) to the National Archives and Records Administration . . . . 68 Fed. Reg. 2101 (Jan. 15, 2003).

[36] 5 U.S.C. § 552a(b)(7).

[37] P.L. 100-503, 5 U.S.C. § 552a note.

[38] 5 U.S.C. 552a(a)(8)(B)(vi).

[39] 20 U.S.C. § 1232g. See CRS Report RL31482, *The Family Educational Rights and Privacy Act of 1974: Recent Developments in the Law.*

[40] P.L. 107-56, 20 U.S.C. § 1232g(j). See CRS Report RL31377: *The USA PATRIOT Act: A Legal Analysis.*

Telecommunications Information.

The Cable Communications Policy Act of 1984. Limits the disclosure of cable television subscriber names, addresses, and utilization information.[41] Cable companies are prohibited from disclosing personally identifiable information concerning a cable subscriber to the government except pursuant to a court order. The order can only be issued if a court finds clear and convincing evidence that the customer was suspected of engaging in a crime and that the information sought was material evidence in the case; and the subject was afforded the opportunity to appear and contest the government's claim. The USA PATRIOT Act of 2001 amended the Cable Act's privacy provision to clarify that it applies only to information about a customer's cable TV service, but not to information about a customer who receives Internet or telephone service from a cable provider. When the government is requesting information about a customer receiving Internet or telephone service from a cable provider, the federal electronic surveillance statutes apply.

The Video Privacy Protection Act of 1988. Regulates the treatment of personally identifiable information collected in connection with video sales and rentals.[42] The Act prohibits videotape service providers from disclosing their customers' names, addresses, and specific videotapes rented or purchased except pursuant to customer consent, or pursuant to a federal or state search warrant, grand jury subpoena, or court order issued to a law enforcement agency. The order can only be issued if a court finds that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. Issuance of court orders requires prior notice to the customer. A court may quash or modify such order if the information or records requested are unreasonably voluminous or if compliance would cause an unreasonable burden on the provider.

Telecommunications Act of 1996. Limits the use and disclosure of customer proprietary network information (CPNI) by telecommunications service providers.[43] The statute does not include specific provisions for the disclosure of CPNI to law enforcement or government officials. Except as required by law or with customer consent, a telecommunications carrier must only use, disclose, or permit access to individually identifiable customer proprietary network information in providing the telecommunications service. Upon customer request, a telecommunications carrier may disclose that customer's proprietary network information to any person designated by the customer. Customer proprietary network information is information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship, and includes information contained in the bills pertaining to telephone exchange service or telephone toll service, but does not include subscriber list information.

---

[41] 47 U.S.C. § 551.

[42] 18 U.S.C. § 2710.

[43] 47 U.S.C. § 222. See CRS Report RL30671, *Personal Privacy Protection: The Legislative Response*.

Health Information.

The Health Insurance Portability and Accountability Act of 1996. HIPAA required publication of a medical privacy rule by the Department of Health and Human Services (HHS) in the absence of a congressional enactment.[44] The final privacy rule, "Standards for the Privacy of Individually Identifiable Health Information," was published in December 2000 and modified in August 2002.[45] Enforcement of the rule goes into effect for the majority of covered entities April 2003. The rule establishes privacy protections for individually identifiable health information held by health care providers, health care plans, and health care clearinghouses. It establishes a series of regulatory permissions for uses and disclosures of individually identifiable health information.[46] Individually identifiable health information is health information created or received by a covered entity (health care provider, health plan, or health care clearinghouse) that relates to past, present, or future physical or mental health or a condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual or there is a reasonable basis to believe that the information can be used to identify the individual. The rule excludes education records covered by FERPA, and employment records held by a covered entity in its role as employer.

The medical privacy rule establishes new procedures and safeguards to restrict the circumstances under which a covered entity may give such information to law enforcement officers. For example, the rule limits the type of information that covered entities may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant. Where state law imposes additional restrictions on disclosure of health information to law enforcement, those state laws continue to apply. This rule sets a national floor of legal protections. In those circumstances when disclosure to law enforcement is permitted by the rule, the privacy rule does not require covered entities to disclose any information. In the event that some other federal or state law requires a disclosure, the privacy rule does not interfere with the operation of those other laws. However, unless the disclosure is required by some other law, covered entities are to use their professional judgment to decide whether to disclose information.

For law enforcement purposes the rule permits disclosure without consent or authorization pursuant to process, and as otherwise required by law.[47] A covered entity may disclose protected health information as required by law;[48] or in

---

[44] P.L. 104-191 § 264, 42 U.S.C. 1320d note.

[45] Standards for the Privacy of Individually Identifiable Health Inforamtion,45 CFR Parts 160 and 164 at [http://www.hhs.gov/ocr/combinedregtext.pdf].

[46] See CRS Report RS20934, *A Brief Summary of the Medical Privacy Rule.*

[47] 45 CFR § 164.512(f).

[48] Required by law means a mandate contained in law that compels a covered entity to make (continued...)

compliance with the requirements of (i) a court order or court-ordered warrant, a judicial subpoena or summons, (ii) a grand jury subpoena, or (iii) an administrative request, including an administrative subpoena or summons, a civil or authorized investigative demand, or similar process authorized under law, provided that the information sought is relevant and material to a legitimate law enforcement inquiry; the request is specific and limited in scope; and de-identified information could not reasonably be used. Covered entities are also permitted to disclose protected health information in the course of judicial and administrative proceedings, and limited information for identification purposes. They are also permitted to disclose information to a law enforcement official about an individual who has died if there is reason to believe the death may have resulted form criminal conduct. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act and implementing authority.[49]

Motor Vehicle Information.

Driver's Privacy Protection Act of 1994. Regulates the use and disclosure of personal information from state motor vehicle records.[50] Personal information is defined as information that identifies an individual, including an individual's photograph, Social Security number, driver identification number, name, address, telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status. Personal information contained in a motor vehicle record may be disclosed for use by any government agency, including any court or law enforcement agency, in carrying out its functions, or to any private person or entity acting on behalf of a Federal, State, or local agency; and for use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, or pursuant to a Federal, State, or local court order.

Communications and Communications Records.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The federal wiretapping and electronic eavesdropping statute permits federal and state law enforcement officers to use wiretapping and electronic eavesdropping under strict limitations.[51] 18 U.S.C. 2510 *et seq*. The federal and state courts may issue interception orders upon applications approved by senior Justice Department or state prosecutors. The applications must demonstrate probable cause to believe that the proposed interceptions will result in the capture of evidence of one or more of statutorily designated crimes. The orders are crafted to minimize the capture of innocent conversations. Officers may share information secured under the orders

---

[48] (...continued)
a use or disclosure or protected health information an that is enforceable in a court of law.

[49] 45 CFR § 164.512(k).

[50] 18 U.S.C. § 2721.

[51] See CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping.*

with other law enforcement or with intelligence officials in connection with the performance of their official duties. Senior Justice Department and state prosecutors may authorize emergency interceptions for 48 hours while an application for a court order is being prepared and presented. Unless postponed by the court for cause, the targets and anyone whose conversations have been captured are entitled to notification within 90 days of the expiration of the order. There are criminal, civil, and administrative sanctions for illegal interception, and evidence secured through an unlawful interception may be declared inadmissible in subsequent judicial or administrative proceedings. See table on "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

The Foreign Intelligence Surveillance Act of 1978. FISA governs the use of wiretapping to collect "foreign intelligence" which is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[52] 50 U.S.C. §§ 1861 *et seq*. The eleven judges of a special court, whose members are assigned from the federal bench, may authorize surveillance upon applications approved by the Attorney General asserting probable cause to belief that the effort will yield foreign intelligence. FISA court surveillance orders are crafted to minimize the capture of conversations not related to foreign intelligence. Officers may share the results with law enforcement officials for the performance of their duties. The Attorney General may authorize emergency surveillance for 72 hours while a FISA order is being secured. The President may authorize surveillance without a court order during time of war or for communications between or among foreign powers. If the government intends to use the results as evidence in judicial proceedings it must inform the parties to the intercepted conversations. Challenges to the legality of the surveillance may be considered ex parte upon petition of the Attorney General. Unlawful surveillance is subject to criminal, civil, and administrative sanctions, and evidence illegally secured may be suppressed.

FISA also empowered judges of the FISA court to issue physical search orders under limitations similar to FISA surveillance orders. In foreign intelligence cases, FISA likewise tracks the procedure used in criminal cases for the installation and use of pen register and trap and trace devices under court order. Finally, it called for FISA orders for the production of tangible items in foreign intelligence and international terrorism investigations. See table on "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

The Electronic Communications Privacy Act of 1986. ECPA amended and augmented Title III. It regulates government access to ongoing and stored wire and electronic communications (such as voice mail or electronic mail), transactional records access, and the use of pen registers, and trap and trace devices.[53] After its

---

[52] See CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework.*

[53] 18 U.S.C. §§ 2510 *et seq.* See CRS Report 98-326, *Privacy: An Overview of Federal* (continued...)

modifications the surreptitious capture of e-mails and other electronic communications in transit enjoy the coverage of Title III and may be accomplished under a Title III court order. When voice mail, e-mails and other electronic communications have been in storage for less than 180 days, they can be seized under a search warrant based on probable cause. Those in storage for 180 days or more can be secured under a court order upon a showing of relevancy and materiality, under a subpoena, or under a search warrant.

ECPA also authorized court orders for the installation and use of pen registers as well as trap and trace devices, which identify source and address of communications, but not the contents of the conversation. These orders may be issued on the basis of relevancy to a criminal investigation and their results need not be disclosed to the individuals whose communications are their targets. Perhaps because in the case of Internet communications header information is more revealing than the mere identification of source and addressee telephone numbers, results of such orders must be reported to the issuing court under seal.

Finally, ECPA established a procedure for government access to the customer records of telephone company or other communications service providers. Here too, access may be had by search warrant, subpoena, or court order (on a showing of relevancy). See "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

The USA PATRIOT Act of 2001. The Act substantively amended Title III of the Omnibus Crime Control and Safe Streets Act, the Electronic Communications Privacy Act, and the Foreign Intelligence Surveillance Act of 1978.[54] The USA PATRIOT Act authorized the disclosure of wiretap and grand jury information to "any federal, law enforcement, intelligence, protective, immigration, national defense, or national security official" for the performance of his duties.[55] It permitted use of FISA surveillance orders when foreign intelligence gathering is "a significant" reason for the order rather than "the" reason. It brought e-mail and other forms of electronic communications within the pen register and trap and trace procedures under both ECPA and FISA. Finally, it authorized FISA orders for access to any tangible item rather than only business records held by lodging, car rental, and locker rental businesses. See table on "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

The Homeland Security Act of 2002. The Act amended Title III of the Omnibus Crime Control and Safe Streets Act, the Electronic Communications

---

[53] (...continued)
Statutes Governing Wiretapping and Electronic Eavesdropping.

[54] P.L. 107-56. See CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping.*

[55] P.L. 107-56, § 202.

Privacy Act, and the Foreign Intelligence Surveillance Act of 1978[56] to authorize sharing the results of the federal government's information gathering efforts under those statutes with relevant foreign, state and local officials. See table on "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

Financial Information. This section provides a description of the Fair Credit Reporting Act, the Right to Financial Privacy Act, and the Gramm-Leach-Bliley Act. The table appended to this report on "Laws Relating to Federal Government Access to Personal Financial Information" also includes the Bank Secrecy Act of 1970, the U.S.A. Patriot Act provisions related to the Financial Crimes Enforcement Network (FinCEN), and relevant provisions of the Tax Reform Act of 1976.

The Fair Credit Reporting Act of 1970. FCRA sets forth rights for individuals and responsibilities for consumer "credit reporting agencies" in connection with the preparation and dissemination of personal information in a consumer report. Under the FCRA, consumer reporting agencies are prohibited from disclosing consumer reports to anyone who does not have a permissible purpose.[57] FCRA covers information gathered by consumer reporting agencies on consumers to evaluate qualifications for credit, employment, insurance, and other transactions; covered information may include identifying (name, address, employer and former address and employer), credit (transactions, etc.), and public record information as well as information on entities seeking credit reports on the consumer. A limited amount of identifying information from a credit bureau's file on a consumer (i.e., "header information" – name, address, employment and previous address) may be disclosed upon request. No notice is required. Consumer reports and any other information in a consumer's file can be disclosed pursuant to a court order or grand jury subpoena; or in connection with the application for a license or for determining eligibility for a government benefit or license. The FBI, for foreign counterintelligence investigative purposes, may obtain names and addresses of financial institutions at which consumers maintain or have maintained accounts, provided the request is signed by an appropriate official who has certified that the investigation is not conducted solely on the basis of activity protected under the First Amendment. The USA PATRIOT Act amended the FCRA to authorize the disclosure of consumer reports and any other information in a consumer's file upon request in writing from any government agency authorized to conduct international terrorism investigations, or intelligence or counterintelligence activities related thereto, stating that such information is necessary for the agency's conduct of that activity and signed by an appropriate supervisor. No notice is required. See table on "Laws Relating to Federal Government Access to Personal Financial Information."

---

[56] P.L. 107-296. See CRS Electronic Briefing Book, *Terrorism – Wiretapping Authority*.

[57] 15 U.S.C. § 1681 *et seq*. See CRS Report RL31666, *Fair Credit Reporting Act: Rights and Responsibilities.*

The Right to Financial Privacy Act of 1978. The RFPA was enacted in response to the 1976 decision of the Supreme Court in *United States v. Miller*,[58] which ruled that individuals have no Fourth Amendment "expectation of privacy" in records maintained by their banks. The RFPA sets forth procedures for the federal government's access to financial institution customer records.[59] RFPA covers the records of individuals who are customers of banks, thrifts, credit unions, credit card issuers, and consumer finance companies. The Act requires the government to present administrative subpoenas or summons based upon reason to believe the information is relevant to a legitimate law enforcement inquiry. In criminal investigations, judicial search warrants based on probable cause must be obtained. Notice to the customer is required except upon issuance of a court order finding the existence of certain exigent circumstances. However, these restrictions do not apply to foreign intelligence activities and investigations related to international terrorism.[60] See "Laws Relating to Federal Government Access to Personal Financial Information."

The Gramm-Leach-Bliley Act of 1999. Requires financial institutions to disclose their privacy policies to their customers.[61] Title V of the Act regulates non-publically available personally identifiable customer (or applicant) information held by "financial institutions," a term that is broadly defined to include anyone in the business of providing services that are financial in nature, including banking, securities, insurance, accounting, tax preparation, asset management, real estate leasing and settlement services. GLBA provides exceptions for law enforcement to the law's general prohibition against "financial institution" sharing of personally identifiable customer information with non-affiliated third parties. Exceptions permit sharing of such information in response to judicial process; as permitted or required under other provisions of law, and in accordance with the Right to Financial Privacy Act; and to provide information to law enforcement agencies, or for an investigation on a matter of public safety. No notice of disclosure to the customer is necessary, except as required pursuant to other law. See table on "Laws Relating to Federal Government Access to Personal Financial Information."

Other Information.

Children's Online Privacy Protection Act of 1998. Requires website operators and online service providers to obtain parental consent to collect a child's personal information, and requires sites collecting information from children to disclose how they plan to use the data.[62] Parental consent is not required for the operator of such a website or online service to collect, use, or disclose such information to respond to judicial process; or to provide information, to the extent

---

[58] 425 U.S. 435 (1976).

[59] 12 U.S.C. § 3401 *et seq*. See CRS Report RS20185, *Privacy Protection for Customer Financial Information.*

[60] 12 U.S.C. § 3414.

[61] P.L. 106-202, 113 Stat. 1338. See CRS Report RS20185, *Privacy Protection for Customer Financial Information.*

[62] 15 U.S.C. § 6501.

permitted under other laws, to law enforcement agencies or for an investigation on a matter related to public safety.[63]

Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations. Revised guidelines were issued by Attorney General Ashcroft in May 2002 which removed prohibitions on the Federal Bureau of Investigation's use of publicly-available sources of information – *e.g.*, libraries or the Internet– except as part of an investigation. The 2002 guidelines authorize the FBI to engage in general topical research, which includes conducting online searches and accessing online sites and forums on the same terms and conditions as members of the public. This will allow the FBI to examine public records, monitor the Internet, survey periodicals and newspapers and commercial databases (like Google or Experian) – not incident to a criminal investigation.[64]

Miscellaneous Provisions. Numerous federal statutes include provisions that regulate the use and disclosure of certain types of information held by the government. For example, the confidentiality and disclosure of tax returns and return information is governed by section 6103 of the Internal Revenue Code,[65] the disclosure of Census data is governed, in part, by 13 U.S.C. § 9 which prohibits the use, publication, or examination of any information collected by the Census Bureau, other than for the statistical purpose for which the information was supplied; records pertaining to the issuance or refusal of visas to enter the United States are governed by 8 U.S.C. 1202(f); release of passport information in passport files is subject to the provisions of the Freedom of Information Act and the Privacy Act, and handled in accordance with the regulations in 22 CFR Part 171 and 172.

Legal Requirements for Warrants, Subpoenas, Court Orders, and Requests

Federal statutes that limit access to records held by third parties often specify the process that the federal government must use to gain access to these records. While the TIA program appears to envision real-time access, if not concurrent access, none of the means currently available to the government for accessing data appear to afford such an open-ended virtual appropriation of databases, either public or private. Leaving aside the question of whether there is sufficient authority for TIA's continuous monitoring of databases, what follows is a description of common tools available to the government to gain access to information.

---

[63] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888 (Nov. 13, 1999) at [http://www.ftc.gov/os/1999/9910/64fr59888.pdf]. See CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation.*

[64] Department of Justice, *Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations* at VI(B). (May 2002). Available at [http://www.usdoj.gov/olp/generalcrimes2.pdf].

[65] 26 U.S.C. § 6103.

Law enforcement officials who seek access to information in records held by third-party custodians have several procedural alternatives that include warrants, grand jury subpoenas, administrative subpoenas, court orders, written requests and oral requests. The complexity of the legal requirements for obtaining warrants, subpoenas, and court orders may be such that TIA would opt for other more expedient avenues of access.[66]

The term "**warrant**" ordinarily refers to a court document, issued by a judge or magistrate pursuant to the demands of the Fourth Amendment, upon the request of a law enforcement officer and without affording other parties an opportunity to object to the issuance or execution of the warrant. A search warrant authorizes a search for evidence in connection with a criminal investigation. Officers seeking a warrant must present sworn statements establishing *probable cause* to believe that the requested search will result in the discovery of evidence of a crime.[67] After the fact, a property owner is entitled to notice that a search has occurred and to an inventory of any property seized.[68] Notice is limited to those who have a reasonable expectation of privacy and under some circumstances this will not include records concerning an individual in a third party's computerized records whose claim to confidentiality has been weakened by making them available to others.[69]

Grand jury subpoena – In the context of its investigation of potential corruption or crime, usually at the request of the prosecuting attorney, the grand jury will issue a subpoena duces tecum – if documents are requested – requiring the record custodian's appearance with the requested documents or records. When subpoena duces tecum are served on record custodians, the government is usually under no obligation to bring the subpoena to the attention of the subject, but the custodian is usually free to do so.

Administrative subpoena – In the context of a civil investigation, an agency pursuant to its statutory authority and in accordance with its rules, may issue a request for information or production of documents, reasonably related to a matter within the jurisdiction of the agency. Generally the subpoena may be challenged in court based on lack of relevance, breadth, or lack of particularity. Often there is no requirement that the subject of the records be notified of the government's request.

Court orders – Generally, parties to litigation have the prerogative of seeking the assistance of the court, through the issuance of an order to produce documents or records or information, to facilitate the discovery process in litigation. In the context of government access to the kinds of information that might be desired for TIA programs two types pf specific court orders, the standards for which are outlined in

---

[66] John Markoff and John Schwartz, *Bush Administration to Propose System for Wide Monitoring of Internet* at A22, New York Times (Dec. 20, 2002).

[67] "Probable cause" means "a fair probability that contraband or evidence of a crime will be found in a particular place," *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

[68] *United States v. Ramirez*, 523 U.S. 65 (1998).

[69] *Cf.*, *United States v. Miller*, 425 U.S. 435 (1976)(no customer expectation of privacy in bank records).

statutes, are particularly relevant: (1) a court ordered electronic surveillance order under the federal wiretap statute, and (2) a surveillance order under the Foreign Intelligence Surveillance Act (FISA). The first may be issued by any federal court, provided the statutory procedures are complied with, including approval by senior federal officials. The second may only be issued by the FISA court. The suspicion threshold varies according to the situation. For example, the federal wiretap statute uses a "probable cause plus" standard,[70] while the court order authorizing installation of a pen register and trap and trace device calls for a finding that the "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."[71] The breadth of access varies from statute to statute as well. Often, the standard of suspicion required for issuance of the order coupled with the type of information sought will define the range of access. In some instances, however, Congress has imposed further limitations. Under the federal wiretap statute, for instance, the authority under the court order terminates as soon as the objectives for which the order was sought have been realized.[72] As noted above, "court order" statutes sometimes limit the manner in which officers may use or disclose such evidence. A few statutes expect court orders to be issued following an adversarial hearing;[73] in others the subject of the records receives notice only after the fact;[74] and in still others there are special provisions for extended postponement of notice under some circumstances.[75] The statute that creates the special court order procedure may indicate the grounds and procedure, if any, under which the subject of a record may seek to bar law enforcement access or use. Some may require prior notice.[76] Where the order is issued and access granted prior to notice, the subject may be limited to the exclusion

---

[70] 18 U.S.C. 2518(3)(the order may be issued "if the judge determines on the basis of the facts submitted by the application that—(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in [18 U.S.C. 2516]; (b) there is probable cause for belief that particular communications concerning that offense will be obtained . . . (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlike to succeed if tried or to be too dangerous; [and] (d) . . . there is probable cause for belief that the facilities from which, or the place where the . . . communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense . . .").

[71] 18 U.S.C. 3123(a); see also, 18 U.S.C. 2703(d)(e-mail records may be disclosed pursuant to a court order when the government "offers specific and articulable facts showing . . . reasonable grounds to believe that the . . . records . . . are relevant and material to an ongoing criminal investigation").

[72] 18 U.S.C. 2518(5).

[73] 42 U.S.C. 290dd-2; 42 C.F.R. §2.64 (disclosure of substance abuse treatment records).

[74] 18 U.S.C. 2518(9)(d)(notice of wiretapping under the federal wiretap statute must be given within 90 days of termination of the tap unless postponed by the court).

[75] 18 U.S.C. 2705 not only permits the court to delay notification of the subject whose e-mail records have been disclosed to the government but empowers the court to forbid the e-mail service provider from tipping off the subject.

[76] 42 C.F.R. §2.64 (substance abuse treatment records).

of evidence or civil remedies to the extent that the application, order, execution of the order, or use of the information fail to meet the requirements of the statute.[77]

An **oral or written request** may procure access based on the consent of the third party information custodian. Issuance of such a request would depend upon the rules and procedures governing the operations of the agent making the request.

Congressional Response

The 108th Congress is likely to reexamine existing federal law in terms of barriers to government access to information necessary to prevent and respond to acts of terrorism; while at the same time insuring that information is maintained in a manner that insures its most effective use, protects against its loss, against inappropriate use or disclosure; ensures public and Congressional scrutiny as a form of checks and balances; and otherwise guarantees individual privacy consistent with the Constitution.

According to Senator Shelby of the Senate Intelligence Committee, "[h]ow broadly it [TIA] will ultimately be used is a matter for policymakers to decide if and when the program bears fruit."[78] On January 13, 2003 Senator Harkin requested that the Defense Appropriations Subcommittee hold hearings on the Total Information Awareness (TIA) project. On January 16, 2003, Senator Russ Feingold introduced S. 188, the Data-mining Moratorium Act, which would limit the use of data mining technology by the Defense Department and by the new Department of Homeland Security without Congressional approval and appropriate civil liberties protections. On January 23, 2003 the Senate passed amendment S.Amdt. 59 (introduced by Senator Wyden) to H.J.Res. 2, the Omnibus Appropriations Act for Fiscal Year 2003, imposing limitations on implementation of Total Information Awareness programs, and requiring a detailed report to Congress. Both the House and Senate approved the FY03 omnibus spending bill, H.J.Res. 2, on February 13, 2003 (P.L. 108-7). It includes in section 111, with slight modifications, the language from S.Amdt 59 regarding the Department of Defense's Total Information Awareness (TIA) program. The bill allows the Administration, 90 days after the bill is enacted to submit a report to Congress on the TIA program, instead of 60 days as proposed by the Senate. The provision has also been modified to clarify that the TIA program may be deployed in the United States to assist in the conduct of lawful U.S. foreign intelligence activities against non-United States persons.

Section 111, Limitation on Use of Funds for Research and Development on Total Information Awareness Program, of H. J. Res. 2 imposes limitations on the use of funds for Total Information Awareness programs. It expresses the sense of Congress that the program should not be used to develop technologies for use in conducting intelligence activities or law enforcement activities against United States

---

[77] *E.g.*, the federal wiretap statute, 18 U.S.C. 2518(10)(suppression of evidence), 2520 (civil damages).

[78] September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Senator Richard C. Shelby Vice Chairman, Senate Select Committee on Intelligence at 42 (December 10, 2002), [http://intelligence.senate.gov/shelby.pdf].

persons without appropriate consultation with Congress, or without clear adherence to principles to protect civil liberties and privacy. It reiterates the primary DOD focus of the Defense Advanced Research Projects Agency. The amendment provides that no funds appropriated or otherwise made available to the Department of Defense, Defense Advanced Research Projects Agency, or to any other department, agency, or element of the Federal Government may be obligated or expended on research and development on the Total Information Awareness program unless a written report, prepared by the Secretary of Defense, the Attorney General, and the Director of Central Intelligence, is submitted to Congress within 90 days after passage of the omnibus spending bill; or the President certifies to Congress in writing that submission of the report to Congress within 90 days is not practicable, and that the cessation of research and development on the Total Information Awareness program would endanger the national security of the United States.

The report to Congress must include a detailed explanation for each project and activity of the Total Information Awareness program – the actual and intended use of funds; the schedule for proposed research and development; and target dates for deployment. It must assess the likely efficacy of systems such as the Total Information Awareness program; the likely impact of the implementation of the Total Information Awareness program on privacy and civil liberties; and provide a list of the laws and regulations that govern the information to be collected by the Total Information Awareness program, and a description of any modifications required to use the information in the manner proposed. The report must include the Attorney General's recommendations for practices, procedures, regulations, or legislation on the deployment, implementation, or use of the Total Information Awareness program to eliminate or minimize adverse affects on privacy and civil liberties.

The amendment prohibits the deployment, implementation, or transfer of the TIA program or a component thereof to any department, agency, or element of the federal government until the Secretary of Defense notifies Congress; and receives from Congress specific authorization for the deployment and a specific appropriation of funds. This limitation does not apply with respect to the deployment or implementation of the Total Information Awareness program, or a component of such program, in support of the lawful military operations of the United States conducted outside the United States, and in support of lawful foreign intelligence activities conducted wholly against non-United States persons.

Another issue that has arisen is whether the Homeland Security Act of 2002 authorizes TIA programs in the newly created Department of Homeland Security (DHS). Although the Homeland Security Act does not expressly authorize Total Information Awareness programs, Congress authorized $500 million for a DHS entity with a name similar to DARPA, Homeland Security Advanced Research Projects Agency (HSARPA). The new law also includes language that authorizes the utilization of data mining and other advanced analytical tools by the new department.[79]

---

[79] P.L. 107-296 §201(d)(14), 116 Stat. 2135, 2147.

Laws Relating to Federal Government Access to Personal Financial Information[80]

Statutory Provision	*Information Sought*	*Process*	*Notice Requirement*
Title V of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801et seq.	Non-publically available personally identifiable customer (or applicant) information held by "financial institutions," a term that is broadly defined to include anyone in the business of providing services that are financial in nature, including banking, securities, insurance, accounting, tax preparation, asset management, real estate leasing and settlement services.	Provides exceptions for law enforcement to the legislation's general prohibition against "financial institution" sharing of personally identifiable customer information with non-affiliated third parties. Exceptions permit sharing of such information: (1) in response to judicial process; (2) as permitted or required under other provisions of law, and in accordance with the Right to Financial Privacy Act; and (3) to provide information to law enforcement agencies, or for an investigation on a matter of public safety.	No notice–except pursuant to other law, such as the Right to Financial Privacy Act.
Right to Financial Privacy Act – 12 U.S.C. §§ 3401 *et seq.*	Records of individuals who are customers of banks, thrifts, credit unions, credit card issuers, and consumer finance companies.	Administrative subpoena or summons–upon reason to believe information is relevant to a legitimate law enforcement inquiry.	Notice required–except upon court order finding the existence of certain exigent circumstances.
"	"	Customer authorization–which must be specific and is limited to a 3-month period.	NA
"	"	Search warrant upon probable cause issued by a judicial officer	

[80] This chart was prepared by M. Maureen Murphy, Legislative Attorney in the American Law Distribution of CRS.

Statutory Provision	*Information Sought*	*Process*	*Notice Requirement*
The Bank Secrecy Act of 1970, 12 U.S.C. §§ 1829b and 1951-1959, and 31 U.S.C. 5311-5322, and its major component, the Currency and Foreign Transactions Reporting Act, 31 U.S.C. §§ 5311-5322 (the anti-money laundering laws). Title III of the USA PATRIOT Act included various amendments to this legislation.	Reports and records of cash, negotiable instrument, and foreign currency transactions of "financial institutions," a term that is defined broadly to include banks, thrifts, credit unions, securities dealers, credit card companies, insurance companies, jewelers, pawnbrokers, travel agencies, loan companies, telegraph companies, money transmitting businesses, and any other business designated by the Secretary of the Treasury. Threshold for reporting currency or foreign transactions is $10,000; geographic targeting orders may be issued lowering that threshold considerably for a limited area and time.	The Secretary of the Treasury may prescribe regulations to insure that adequate records are maintained of transactions that have a "high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." 12 U.S.C. § 1829b. These records may be subpoenaed. Institutions must develop anti-money laundering programs. Banks, thrifts, and credit unions; money service businesses (including informal networks such as hawalas); casinos and card clubs; and securities firms must file suspicious activities reports (SAR's).	No notice.
USA-PATRIOT Act, 31 U.S.C. § 310. Statutory authority for the Financial Crimes Enforcement Network (FinCEN).	This is a government-wide data access service to identify possible criminal activity, support investigations, identify potential violations of the anti-money laundering laws, determine emerging trends in money laundering and financial crimes, support intelligence or counter intelligence initiatives, and furnish law enforcement authorities with information to aid in detecting and preventing terrorism,	FinCEN collects data reported under the anti-money laundering laws; currency flow information; records and data maintained by federal, state, local and foreign agencies; and other privately and publicly available information. It analyzes this information and disseminates the results and supports and fosters federal and international efforts against financial crimes.	No notice.

Statutory Provision	*Information Sought*	*Process*	*Notice Requirement*
	financial crimes, and other criminal activity.		
Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.* Information gathered by consumer reporting agencies on consumers to evaluate qualifications for credit, employment, insurance, other transactions; may include identifying (name, address, employer and former address and employer), credit (transactions, etc.), and public record information as well as information on entities seeking credit reports on the consumer.	Limited amount of information from credit bureau's file on a consumer–i.e., "header information," identifying information–name, address, employment and previous address and employment to a government agency.	Upon request.	No notice.
Fair Credit Reporting Act, 15 U.S.C. § 1681v.	Consumer reports and any other information in a consumer's file.	Pursuant to a court order or grand jury subpoena. In connection with the application for a license or for determining eligibility for a government benefit or license. One court has ruled that the Federal Trade Commission, as the enforcement agency for the legislation, may cause a consumer reporting agency to produce its complete files on a consumer or consumers pursuant to an agency subpoena. *FTC v. Manager, Retail*	

Statutory Provision	*Information Sought*	*Process*	*Notice Requirement*
		Credit Co., 515 F. 2d 988 (D.C. Cir. 1975). The FBI, for foreign counterintelligence investigative purposes, may obtain names and addresses of financial institutions at which consumers maintain or have maintained accounts, provided the request is signed by appropriate official who has certified that the investigation is not conducted solely on the basis of activity protected under the First Amendment.	
Fair Credit Reporting Act, as amended by the USA PATRIOT, Act, 15 U.S.C. § 1681v.	Consumer reports and any other information in a consumer's file.	Upon request in writing from any government agency authorized to conduct international terrorism investigations, or intelligence or counterintelligence activities related thereto, stating that such information is necessary for the agency's conduct of that activity and signed by an appropriate supervisor.	No notice.
Tax Reform Act of 1976, as amended by the Tax Equity and Fiscal Responsibility Act of 1982, 26 U.S.C. §§ 7602, 7609, and 7610.	Confidential records of individuals and other legal entities that are held by financial institutions, and other third-party record keepers, e.g., lawyers, accountants, consumer reporting agencies, accountants, and credit card issuers.	Internal Revenue Service summons.	Notice is required and must be followed by a waiting period during which the persons whose records are requested may challenge the summons in court.

Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act[81]

Applicable Law	*Coverage*	*Purpose for Access*	*Process*	*Notice Requirement*
Fourth Amendment:	Information and data in which the target of the search (i.e., the subject of the criminal investigation) has legitimate expectation of privacy (i.e., one that the courts will protect because it comports with Fourth Amendment case law).	Seeking evidence of a crime.	Judicial search warrant issued upon probable cause.	Contemporaneous notice of seizure.
"	"	Varying governmental purposes and circumstances (criminal evidence, inspections, border search, exigent circumstances, etc.).	Fourth Amendment warrant, probable cause, and possibly notice requirements may be eased under special circumstances.	Delayed in some instances.
Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1861.	Tangible items–including books, records, documents, and papers.	Seeking foreign intelligence information (not involving a U.S. person) or information to protect against international terrorism or clandestine intelligence	FISA court or magistrate order for access, following an FBI supervisor-approved application specifying the foreign intelligence or anti-terrorism purposes.	Disclosure prohibited.

[81] This chart was prepared by Charles Doyle, Senior Specialist in American Public Law, American Law Division of CRS.

Applicable Law	*Coverage*	*Purpose for Access*	*Process*	*Notice Requirement*
		(spy) activities.		
Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1821-1828.	Physical searches.	Seeking foreign intelligence information, including tangible or intangible items (no longer needs to be sole purpose; need only be measurable purpose with criminal investigative purposes permitted).	FISA court order issued upon application approved by the Attorney General showing probable cause to believe that target is a foreign power or agent and owner of the searched property. Process is subject to standards designed to minimize unnecessary intrusions into matters of U.S. persons and to limits on duration of the order. Legality of seizures under this process is to be tested in an ex parte proceeding; evidence obtained through this process may be shared with law enforcement authorities investigating criminal activity. Emergency orders may be issued by the Attorney General, which must be approved by the FISA court to which application must be made within 72 hours. If there is no FISA court approval, results may be used only with the Attorney General's approval and only in cases involving a threat of death or serious bodily injury. U.S. persons may not to targeted based solely on their exercise of 1st Amendment rights.	U.S. persons whose residences were searched are notified any time if the Attorney General determines that national security interests do not require secrecy. If the U.S. intends to use evidence obtained from a physical search, it must provide notification to the aggrieved prior to the proceeding in which it will use it.
Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1822.	Physical searches directed at information or property exclusively of foreign powers.	Seeking tangible or intangible items for foreign intelligence purposes.	Presidential directive through the Attorney General for searches without a court order for up to one year. Certification of minimization procedures sent under seal to the FISA court.	No statutory requirement.
Foreign Intelligence Surveillance Act of 1978, 50 U.S.C.	Physical searches.	Seeking tangible or intangible items for foreign intelligence	The President may order a physical search for up to 15 days during a time of declared war.	No statutory requirement.

Applicable Law	*Coverage*	*Purpose for Access*	*Process*	*Notice Requirement*
1829.		purposes in time of war.		
Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1801-1810.	Communications using wire or radio facilities.	Seeking foreign intelligence information (no longer need to sole purpose; need only be measurable purpose with criminal investigative purposes permitted).	FISA court order issued upon application approved by the Attorney General showing probable cause to believe that target is a foreign power or agent. Process is subject to standards designed to minimize unnecessary intrusions into matters of U.S. persons and to limits on duration of the order. Legality of surveillance under this process is to be tested in an ex parte proceeding; evidence obtained through this process may be shared with law enforcement authorities investigating criminal activity. Emergency orders may be issued by the Attorney General, which must be approved by the FISA court to which application must be made within 72 hours. If there is no FISA court approval, results may be used only with the Attorney General's approval and only in cases involving a threat of death or serious bodily injury. U.S. persons may not be targeted based solely on their exercise of 1st Amendment rights.	U.S. persons subjected to surveillance are notified at any time the Attorney General determines that national security interests do not require secrecy. If the U.S. intends to use evidence obtained from a physical search, it must provide notification to the aggrieved prior to the proceeding in which it will use it.
Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1811.	Communications using wire or radio facilities.	Seeking tangible or intangible items for foreign intelligence purposes in time of war.	The President may order surveillance for up to 15 days during a time of declared war.	No statutory requirement.
Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1802.	Communications exclusively among or between foreign powers using wire or radio	Seeking tangible or intangible items for foreign intelligence purposes.	Presidential directive through the Attorney General for surveillance without a court order for up to one year. Certification of minimization procedures sent under seal to the FISA court.	No statutory requirement.

Applicable Law	*Coverage*	*Purpose for Access*	*Process*	*Notice Requirement*
	facilities.			
18 U.S.C. 2510-2522 ("Title III").	Wire (phone), oral (face to face), or electronic (nonverbal) surveillance (conversations captured by machine or device).	Seeking evidence of a crime.	Consent of one party to the communication.	No notice required.
18 U.S.C. 2510-2522 (Title III).	Wire (phone), oral (face to face), or electronic (nonverbal) surveillance (conversations captured by machine or device.	Seeking evidence of a crime.	Federal or state court order issued on application approved by senior prosecutorial authorities showing probable cause pertaining to a limited list of predicate offenses. Process is subject to standards designed minimize the capture of unrelated (not crime related) conversations. Legality of surveillance under this process is tested in suppression hearings if the government seeks to use the resulted in a judicial or administrative proceeding; evidence may be shared with law enforcement or intelligence authorities for the performance of their duties. Emergency orders may be issued by senior prosecutorial authorities, which must be approved by the court to which applications must be made within 48 hours. If there is no court approval, results are inadmissible.	Targets of the interception and those whose conversations have been captured are notified within 90 days after expiration of the court order authorizing the surveillance, unless the court postpones notification for cause.
18 U.S.C. 2701-2711(relating to communications records and stored communications).	Wire and electronic communications content in storage less than 180 days.	Seeking evidence of a crime.	Search warrant issued upon probable cause.	Court may bar notice to the customer under exigent circumstances.
18 U.S.C. 2701-	Wire and electronic	Seeking evidence of a	Search warrant issued upon probable cause; court order	Court may bar

Applicable Law	*Coverage*	*Purpose for Access*	*Process*	*Notice Requirement*
2711(relating to communications records and stored communications).	communications content in storage more than 180 days.	crime.	upon relevancy and materiality; or grand jury, trial, or administrative subpoena upon relevancy.	notice to the customer under exigent circumstances.
18 U.S.C. 2701-2711(relating to communications records and stored communications).	Wire and electronic communications records.	Seeking evidence of a crime.	Search warrant issued upon probable cause; court order upon relevancy and materiality; or grand jury, trial, or administrative subpoena upon relevancy.	Court may bar notice to the customer under exigent circumstances.
18 U.S.C. 2709 (relating to counterintelligence access to communications records.	Wire and electronic communications records.	Seeking information relevant to international terrorism or foreign spy investigations.	Written request from senior FBI officials certifying relevancy. Disclosure only to federal agencies.	No notice; disclosure outside federal agencies is forbidden.
18 U.S.C. 2701-2711(relating to communications records and stored communications).	Wire and electronic communications content or records.	Seeking evidence of a crime.	With customer consent; for service related or service provider protection purposes; threat of serious injury; evidence of crime inadvertently discovered by service provider (content only); written request concerning telemarketing fraud (records only).	Except for access based on customer consent, no statutory notice requirement.
18 U.S.C. 3121-3127 (pen registers; trap and trace devices).	Source/address information for wire and electronic communications.	Seeking evidence of a crime.	Court order for the installation and use of pen register and/or trap and trace devices on the basis of relevancy for 60 days (renewable). The results in cases involving the Internet must be reported to the court under seal after termination. Senior Justice Department officials may approve emergency installation and use (for 48 hours pending the	The court may forbid disclosure; otherwise no statutory provision.

Applicable Law	*Coverage*	*Purpose for Access*	*Process*	*Notice Requirement*
			application for a court order) in the face of threats of serious injury, or in organized crime cases, national security cases, or felonious attacks on computers.	
50 U.S.C. 1841-1846 (pen registers; trap and trace devices).	Source/address information for wire and electronic communications.	Seeking information on international terrorism or foreign spy activities.	FISA court order for the installation and use of pen register and/or trap and trace devices on the basis of relevancy for 90 days (renewable). The Attorney General may approve emergency installation and use (for 48 hours pending the application for a court order). U.S. persons may not to targeted based solely on their exercise of 1st Amendment rights. Process is subject to standards designed to minimize unnecessary intrusions into maters of U.S. persons and to limits on duration of the order. Legality of this process is to be tested in an ex parte proceeding; evidence obtained through this process may be shared with law enforcement authorities investigating criminal activity.	The court may forbid disclosure, but aggrieved persons must be notified if the government intends to use the results as evidence.
Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1845.	Source/address information for wire and electronic communications.	Seeking information relevant to international terrorism or foreign spy investigations.	The President may order installation and use of a pen register and/or a trap and trace device for up to 15 days during a time of declared war.	No statutory requirement.