Recent Privacy Developments in the United States, Particularly with Respect to Travelers Using Air Transport

Marc Rotenberg
President, Electronic Privacy Information Center (EPIC)
Adjunct Professor, Georgetown University Law Center

Washington, DC

21 March 2007

Overview

In early 2007, a wide range of privacy issues are under debate in the United States. Recent reports about the abuse of Patriot Act authorities by the FBI have raised further questions about the adequacy of the oversight mechanisms that were created when new police powers where established after 9-11. The proposal to create a national identification system through the implementation of the REAL ID Act has also sparked opposition from political leaders in both parties as well as state governments.

At the same time, legislation is moving forward in Congress that would establish independence for the Privacy and Civil Liberties Oversight Board that currently reports to the President, as well as establish new reporting requirements for data mining activities within the federal government.

With respect to the privacy of travelers, much of the focus continues to be on problems with the watch list systems as well as proposals to expand profiling and screening of air travelers. The Secure Flight program was delayed because of flaws. Expansion of US-VISIT, the border control system, continues, though the proposal to use contactless RFID identity documents for foreign visitors has been withdrawn. Debate surrounds the terrorist risk profile ratings assigned to all international travelers by the Automated Targeting System, operated by the Customs and Border protection agency, as well as the adequacy of the recently announced redress procedures for those travelers who are placed on government watch lists.

The change in political control in the United States Congress has begun to restore some of the checks and balances of the federal government. New Committee Chairmen have the authority to conduct more vigorous oversight and to pursue legislative proposals that have stalled in previous sessions of Congress. Senator Patrick Leahy, the new Chairman of the Senate Judiciary Committee, has indicated that the restoration of privacy, the repair of a broken oversight process and the return of accountability will be top priorities for the Senate Judiciary Committee in the new Congress. At a speech at the Georgetown University Law Center, Senator Leahy warned that the "Administration as rolled back open government laws and systematically eroded Americans' privacy rights. It has brazenly refused to answer the legitimate oversight questions of the public's duly elected representatives, and it has acted outside lawful authority to wiretap Americans without warrants, and to create databanks and dossiers on law-abiding Americans without following the law and without first seeking legal authorization." [1] Rep. Bennie Thompson, Chairman of the Committee on Homeland Security, has expressed concern

[1] Senator Patrick Leahy, "Ensuring Liberty And Security Through Checks And Balances: A Fresh Start For The Senate Judiciary Committee In The New 110th Congress," (Dec. 13, 2006), http://leahy.senate.gov/press/200612/121306.html

about a range of programs operated by the Department of Homeland Security, including the Automated Targeting System.[2]

General Privacy Matters

Implementation of REAL ID Act. In 2005, Congress enacted the REAL ID Act, which will require the state agencies charged with the issuance of driver's licenses and identity documents to adopt federal standards. This will enable the integration of federal databases through a new system of national identification and more frequent requirements for personal identification in the United States. Personal information will be kept in a database network that would be accessible by motor vehicle departments nationwide. Eventually, all Americans would be required to obtain a "REAL ID." Those without one would be barred from federal buildings or airplanes unless they could show a passport or some other form of federally approved photo identification. The measure was passed without a public hearing or a recorded vote.

In February 2007, almost two years after passage of the Act, the Department of Homeland Security issued draft regulations.[3] The Department of Homeland Security Data Privacy and Integrity Advisory Committee also held a public hearing to discuss the proposed regulations.[4] However, public opposition to REAL ID remains strong with state governments expressing particular concern about the cost, which is estimated to exceed $ 23 billion. As a consequence, the White House announced on March 2, 2007 that the implementation of REAL ID will be delayed until at least the end of 2009.[5]

Establishment of Independent Privacy Agency. The Intelligence Reform and Terrorism Prevention Act of 2004 established the Privacy and Civil Liberties Oversight Board. The Privacy Board consists of five members appointed by and serving at the pleasure of the

---

[2] Comments of Rep. Bennie G. Thompson, on the Privacy Act Systems Record Notice for the U.S. Customs and Border Protection Automated Targeting System, at 6 (Dec. 8, 2006) ("The automated risk assessment process itself also suffers from lack of transparency. Beyond checking identities against watch lists, which would obviously flag a high risk passenger, the process and data points for flagging passengers for greater CBP scrutiny based on a computerized "risk assessment" that remains invisible to the public. As such, it has stirred understandable anxiety among citizens who have no way of assessing the objectivity or reliability of the process, which has been described as everything from data-mining to risk-scoring in the press.")

[3] "DHS: DHS Issues Proposals for States to Enhance Driver's Licenses," (Mar. 1, 2007), http://www.dhs.gov/xnews/releases/pr_1172765989904.shtm.

[4] "DHS Data Privacy and Integrity Committee Meeting Information," (Mar. 21, 2007), http://www.dhs.gov/xinfoshare/committees/gc_1161274938888.shtm

[5] "Real ID Act postponed two years: The 2005 law requiring new driver's licenses now won't take effect until 2009," *The Los Angeles Times*, Mar. 2, 2007, http://www.latimes.com/news/printedition/asection/la-na-realid2mar02,1,5780163.story?coll=la-news-a_section%3A&ctrack=1&cset=true

President. The Board is part of the White House Office within the Executive Office of the President and supported by an Executive Director and staff. The Board advises the President and other senior executive branch officials presumably to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism. This includes advising on whether adequate guidelines, supervision, and oversight exist to protect these important legal rights of all Americans.[6] However, the board typically meets in secret, provides no public reports or analyses, and notably supported the President's domestic surveillance program, which permits the interception of domestic communications of US citizens without judicial approval.[7] Privacy experts have recommended stronger oversight mechanisms consistent with the recommendations of the 9-11 Commission Report.[8]

Now, lawmakers want to replace the White House privacy and civil liberties board created by Congress in 2004 with one that is more independent of the president.[9] Sen. Joseph I. Lieberman (I-Conn.), the chairman of the Homeland Security and Governmental Affairs Committee and Rep. Bennie Thompson (D-Miss.), chairman of the House Homeland Security Committee, have expressed concern that the Privacy Oversight Board has been largely ineffective. Title VIII of the Implementing the 9/11 Commission Recommendations Act of 2007 would strengthen the Privacy Board by making it an independent agency, requiring Senate confirmation of all members, and establishing subpoena authority and reporting requirements.[10] The measure passed the House of Representatives on January 9, 2007. Similar legislation has passed in the Senate on March 13, 2007.[11] However, it is possible that the President will veto the legislation because of a provision to grant agency employees limited collective bargaining rights. The President has said that this would curb needed flexibility at the U.S. Transportation Security Administration and diminish traveler safety.[12]

---

[6] The White House, "Privacy and Civil Liberties Oversight Board," http://www.whitehouse.gov/privacyboard/

[7] "Oversight board briefed on NSA surveillance: Some impressed by 'how careful' the government is in protecting privacy," Associated Press, Nov. 28, 2006, http://www.msnbc.msn.com/id/15932976/

[8] Marc Rotenberg, "The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11," *Social Science Research Network Working Paper Series* (Sept. 2006), http://epic.org/epic/ssrn-id933690.pdf

[9] "Congress Seeks 'Bite' for Privacy Watchdog," *The Washington Post*, at D1, Feb. 13, 2007.

[10] The Library of Congress: Thomas, "H.R.1: Implementing the 9/11 Commission Recommendations Act of 2007 (Engrossed as Agreed to or Passed by House)," http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.+1:

[11] The Library of Congress: Thomas, "S.4: Improving America's Security by Implementing Unfinished Recommendations of the 9/11 Commission Act of 2007 (Reported in Senate)," http://thomas.loc.gov/cgi-bin/query/D?c110:2:./temp/~c110m5X5Kq::

[12] "White House threatens to veto 9/11 bill," *Reuters*, Feb. 28, 2007.

Abuse of Patriot Act. The Patriot Act significantly expanded the FBI's authority to obtain information through National Security Letters, a procedure that compels the production of records held by private entities, such as banks, telephone companies, and universities, without judicial review. Section 505 of the Patriot Act broadened the FBI's authority by eliminating the requirement that the information sought in an NSL must pertain to a foreign power or an agent of a foreign power. The change also permits Special Agents in charge of the FBI's 56 field offices to signs NSLs, a change that significantly expanded approval authority. In addition, the Patriot Act created a new authority permitting the FBI to use NSLs to obtain full consumer credit reports in international terrorism investigations. [13]

An extensive report on the use of National Security Letter authority, released on March 9, 2007 by the Office of the Inspector General of the Department of Justice, found far-reaching problems with the reporting to Congress and the conduct of searches. First, the report found that the total number of NSL requests that were reported to Congress in 2003, 2004, and 2005 were significantly understated.[14] The Inspector General's report estimated that approximately 8,850 NSL requests, or 6 percent of NSL requests issued by the FBI during this period, were missing from the database. The report also found several instances of improper or illegal use of National Security Letter authorities.[15] In addition to 26 possible violations of law that were reported by the FBI General Counsel to the Intelligence Oversight Board, the Inspector General also found that 22 percent of the investigative files reviewed contained one or more IOB violations that were not reported to the FBI General Counsel or the Intelligence Oversight Board.[16] The possible IOB violations fell into three categories: improper authorization for the NSL, improper requests under the pertinent national security letter statutes, and unauthorized collections.

Both the Senate Judiciary Committee and the House Judiciary Committee held hearings in March 2007 to review the report of the Inspector General regarding the National Security Letter authority. The FBI acknowledged that there has been "inadequate auditing and oversight" of National Security Letter authority.[17]

Data Mining. A report from the Congressional Research Service in January 2007 raised new questions about the extent of data mining in the federal government.[18] Concern has also been raised about the ADVISE ("Analysis, Dissemination, Visualization, Insight and

---

[13] Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of National Security Letters," (Mar. 2007), http://www.usdoj.gov/oig/special/s0703b/final.pdf

[14] *Id*. at xvii.

[15] Id. at xxviii.

[16] *Id.* at xxxi.

[17] FBI, "Response to DOJ Inspector General's Report on FBI's Use of National Security Letters," (Mar. 9), http://www.fbi.gov/pressrel/pressrel07/nsl030907.htm

[18] Congressional Research Service Report, "Data Mining and Homeland Security: An Overview" (Jan. 18, 2007), http://www.fas.org/sgp/crs/homesec/RL31798.pdf

Semantic Enhancement") program, which collects and analyze vast amounts of information on typical Americans.[19] The Homeland Security Department began developing ADVISE in 2003, the same year that Congress cancelled funding for another extensive data mining program Total Information Awareness over privacy concerns. Legislation was introduced in the Senate that would require annual public reports from "the head of each department or agency of the Federal Government that is engaged in any activity to use or develop data mining . . ." The Federal Data Mining Reporting Act of 2007 was included in S. 4, which passed the Senate on March 13, 2007.

Information Sharing Environment. Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 set out the framework to establish the Information Sharing Environment in the federal government. The law grants the President authority to "create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[20] The White House has issued a Memorandum for the Heads of Executive Departments and Agencies setting out Guidelines and Requirements in Support of the Information Sharing Environment.[21] The Guidelines make clear that there is an obligation to "protect the information privacy rights and other legal rights of Americans."[22] However, the privacy rules that followed from the Guidelines were harshly criticized by privacy experts as undermining both statutory and Constitutional protections for privacy.[23] The Privacy Guidelines for the Information Sharing Environment do not provide legal protections for non-Americans.

Traveler Privacy

Automated Targeting System. In December 2006, it was reported that a system designed to assign risk ratings to cargo entering the United States was also being used to assign terrorist ratings to travelers. Such profiling of travelers would violate section 514 of the Department of Homeland Security Appropriations Act. According to one report, "The Homeland Security Department's newly revealed computerized risk assessments of international travelers may violate a specific ban that Congress imposed as part of the agency's budget over the past three years." [24] The U.S. Customs and Border Protection

---

[19] "New Profiling Program Raises Privacy Concerns," *The Washington Post,* Feb. 28, 2007, at D3, http://www.washingtonpost.com/wp-dyn/content/article/2007/02/27/AR2007022701542.html

[20] Sect. 1016(b)(1). See generally, Office of the Director of National Intelligence, "Information Sharing Environment: Implementation Plan," (Nov. 2006), http://www.dni.gov/press_releases/ISE-impplan-200611.pdf

[21] Available at http://www.fas.org/sgp/news/2005/12/wh121605-memo.html.

[22] Sect. 2(e).

[23] "Civil Libertarians Protest Privacy Policy: New Guidelines Do Little to Protect Established Rights, White House Board Told," The Washington Post, Dec. 6, 2006, at A11, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/05/AR2006120501287.html

[24] "Traveler Risk System May Violate Ban," Associated Press, Dec.7, 2006.

agency disputes this interpretation of the law.[25] The Department of Homeland Security has described the Automated Targeting System as "one of the most advanced targeting systems in the world."[26]

Delay of Secure Flight. The Transportation Security Administration is developing a passenger pre-screening program called "Secure Flight."[27] According to the agency, Secure Flight involves the submission of a limited amount of passenger reservation information by an aircraft operator to TSA for watch list matching purposes. However, implementation of Secure Flight will be delayed until 2010, at least five years behind schedule, according to the head of the Transportation Security Administration. Secure Flight was suspended a year ago after two government reports detailed security and privacy problems. One report found 144 security vulnerabilities.[28] About $140 million has been spent on the program, and the TSA is seeking another $80 million for proposed changes.

Registered Traveler. The Transportation Security Administration and private industry are developing the Registered Traveler program to provide expedited security screening for passengers who volunteer biometric and biographic information to a TSA-approved Registered Traveler vendor and successfully complete a security threat assessment.[29] According to a recent statement by the TSA, the agency expects to be ready to begin screening Registered Traveler program applicants in mid-June.[30]

US-VISIT. The most elaborate system of border security in the United States is the US-VISIT program. The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is an integrated government-wide program intended to improve the nation's capability to collect information about foreign nationals who travel to the United States, as well as control the pre-entry, entry, status, and exit of these travelers.[31] Along with integrating various databases containing visitor information, US-VISIT also scans,

---

[25] "Facts Concerning the Automated Targeting System – CBP.gov," Dec. 8, 2006, http://www.cbp.gov/xp/cgov/newsroom/highlights/cbp_responds/facts_automated_targeting_sys.xml

[26] Dept. of Homeland Security, "Privacy Impact Assessment for the Automated Targeting System," (Nov. 22, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf

[27] Transportation Security Administration, "TSA: Secure Flight Program," http://www.tsa.gov/what_we_do/layers/secureflight/editorial_1716.shtm.

[28] Government Accountability Office, "Aviation Security Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program," (Feb. 9, 2006), http://www.gao.gov/new.items/d06374t.pdf

[29] Transportation Security Administration, "TSA: Registered Traveler," http://www.tsa.gov/what_we_do/layers/rt/index.shtm

[30] Transportation Security Administration, "TSA: Testimony by Kip Hawley" (Feb. 9, 2006), http://www.tsa.gov/press/speeches/speech_1002.shtm

[31] EPIC, "EPIC US-VISIT Page," http://www.epic.org/privacy/us-visit/

collects and uses biometric identifiers of visitors to the United States. An inkless fingerprinting system captures both of a visitor's index fingerprints and a digital photograph is taken. U.S. Customs and Border Protection officers compare the biometric information to travel documents and other information in US-VISIT databases. If a visitor refuses to provide fingerprints or be photographed, he generally is not permitted to enter the country. Data elements used by US-VISIT include the information made available through arrival and departure manifests. This information includes complete name, date of birth, citizenship, sex, passport number and country of issuance, country of residence, United States visa number, date, place of issuance (where applicable), alien registration number (where applicable), address while in the United States, and such other information that the Attorney General, in consultation with the Secretaries of State and Treasury, deems necessary for the enforcement of the immigration laws and to protect safety and national security.[32] The Department of Homeland Security recently announced that it has abandoned plans to use radio frequency identification (RFID) technology in the US-VISIT border security system after pilot testing failed.[33] The announcement followed a report from the Government Accountability Office that found numerous performance and reliability programs in the 15-month test.[34]

Establishment of Traveler Redress Procedures. The Department of Homeland Security recently announced that it would launch the Traveler Redress Inquiry Program (TRIP). DHS described TRIP as "a central gateway to address watch list misidentification issues, situations where individuals believe they have faced screening problems at immigration points of entry, or have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at our nation's transportation hubs."[35] DHS also indicated that it will "share information it receives with the Department of State and airport and airline operators, as needed, to resolve issues."[36] However, privacy experts have questioned the adequacy of the program and recommended instead that all government record-keeping systems, including the no-fly and selectee lists, comply with the full requirements of the Privacy Act.[37] According to the Electronic Privacy Information Center (EPIC), "If a person is placed on one of these watch lists, he should know why and be able to challenge the determination. Denying citizens the right to ensure that the system contains accurate, relevant, timely and complete records will

---

[32] *Id.*

[33] Hearing on Homeland Security Budget, House Committee on Homeland Security, (Feb. 9, 2007), http://www.epic.org/privacy/us-visit/chertoff_020907.pdf

[34] Government Accountability Office, "Border Security: US-VISIT Program Faces Strategic, Operational and Technological Challenges at Land Ports of Entry," (Jan. 31, 2007), http://www.gao.gov/new.items/d07378t.pdf

[35] "DHS: DHS to Launch Traveler Redress Inquiry Program," (Jan. 17, 2007), http://www.dhs.gov/xnews/releases/pr_1169062569230.shtm

[36] *Id.*

[37] EPIC, "Spotlight on Surveillance: Problem-Filled Traveler Redress Program Won't Fly," (Nov. 2006), http://epic.org/privacy/surveillance/spotlight/1106/default.html

increase the probability that the watch lists will be an error-prone, ineffective means of targeting individuals as they seek to exercise a variety of rights and privileges."

Deployment of Backscatter X-Ray in U.S. Airports. As part of the effort to screen airline passengers, he United States has begun the deployment of a technology that provides TSA officials with images of travelers as if they were naked.[38] As a privacy measure, the TSA said it had worked with industry specialists to blur any images of body parts generated by the scan, and likened the resulting picture to a "chalk outline" of a person. But privacy experts have cautioned that the device is essentially a digital camera that would allow the agency to store and record the original, unobscured image.[39] The TSA will test the machine at Phoenix Sky Harbor International Airport for 60 to 90 days before deploying machines in Los Angeles and New York's John F. Kennedy Airport for additional testing this year.

[38] Reuters, "Critics: New airport x-ray is virtual strip search," Feb. 24, 2007," http://news.com.com/Critics+New+airport+X-ray+is+a+virtual+strip+search/2100-1008_3-6161954.html

[39] "X-ray tests both security, privacy," *USA Today*, Dec. 26, 2006, http://www.usatoday.com/news/nation/2006-12-26-backscatter_x.htm?csp=34.