The "Positive Profiling" Problem: Learning from the U.S. Experience

Why adoption of airline data passenger data profiling has not worked in the United States

A joint report from
The American Civil Liberties Union and Privacy International

October 2006

Summary

Far too many efforts to combat terrorism have focused on the use of sensitive personal information and mass surveillance - techniques that have been demonstrated to deliver limited benefits and that create substantial negative outcomes. Much of the responsibility for this approach to anti-terror policy belongs to the U.S. Government. The EU however is not exempt from this type of policy, however. For a number of years the European Union and its Member States have been implementing expansive data surveillance policies that in many ways mimic U.S. policies and in some particular ways go well beyond what is considered acceptable in the U.S.

We noticed a resurgence of this trend after the security alert in August 2006 upon the arrests in Britain that broke up a suspected plot to target transatlantic air travel. Immediately across Europe we saw a surge of commentary from the media, experts, and policy-makers on the need for *positive profiling* of passengers and expanded surveillance techniques to detect terrorists. This led eventually to reduced protections over passenger data protections to the U.S., renewed calls from U.S. authorities for extended access to this data, and calls within the EU to accelerate policy-making to ensure that EU authorities are granted powers to access and process passenger data.

Nearly everyone presumed that *positive profiling* actually existed, was operational, and was a reasonable response to increased concerns about security. In fact, the very definition of 'profiling' is unknown and its practical application is quite limited. Technologically it is not only impractical to implement but it is also politically unpalatable.

Contrary to the understanding of some in Europe, the United States government currently does not have in place a system for the systematic examination of air travellers' personal data on domestic flights. As Europeans well know, the U.S. government requires passenger name records (PNR) for each passenger for flights into and over the United States. But it does not do this on domestic flights.

The United States does have in place a rudimentary system called Computer-Aided Passenger Pre-Screening System (CAPPS). This system, which is administered not by the government but by the airlines, examines a few basic attributes of passenger reservations, such as whether the passenger paid cash and bought a one-way ticket (though not all the factors are public). This system has been in place since the 1990s, but is considered rudimentary and inadequate by the government.

The absence of a *positive profiling* system in the United States is not through lack of intent. Since 2002, the Bush Administration has been pushing for the creation of a new system for such profiling. However, implementation is still highly uncertain, and for very good reasons.

This report looks into the challenges encountered by the Bush Administration in its efforts to establish a mass-surveillance scheme. These challenges are a mix of technological, political, legal, and social influences that have prevented the development of a profiling scheme. We wonder why, despite the internal policy struggles in the U.S., these policies seem to be re-appearing as uncontroversial elsewhere.

As the European Union and its Member States implement schemes for mass surveillance of movement and at borders, policy-makers must learn from prior mistakes in judgement rather than merely replicating them.

Timeline for Profiling Problems

2002 - The Rise of CAPPS II and the Rise of Delays

- In February 2002, the media reported that the U.S. government was working on a system for pulling together travel histories and a potentially wide array of other personal information on each traveller, and using data mining and predictive software to evaluate potential terrorist threats among the general population. Under the system, dubbed CAPPS II, each flyer would be assigned a code of red, yellow, or green, which determined their treatment at security.[1]
- The system immediately created a firestorm as critics on both the left and the right, as well as in the travel industry, complained that the system would constitute an enormous invasion of privacy and lead to unfair targeting of innocent individuals without recourse.
- In a May 2002 report to Congress, the Transportation Security Administration (TSA) promised that it would begin testing the system in the fall.
- In September 2002, the Washington Post reported that CAPPS II was months behind schedule, and that supporters in Congress were uneasy that the TSA had not even begun a pilot program.[2]

2003 - Political and Legal Challenges Emerge

- In January 2003, the TSA issued a notice in the Federal Register, as required by the Privacy Act, outlining its plans for the giant new databases that CAPPS II would require.
- In February 2003, TSA officials announced that the agency would begin tests of the system the very next month, in March 2003.
- In March 2003, the TSA declared that it "expects to test CAPPS II this spring and implement it throughout the U.S. commercial air travel system by the summer of 2004."[3]

[1] Robert O'Harrow, "Intricate Screening of Fliers in Works," *Washington Post*, Feb. 1, 2002; online at http://www.washingtonpost.com/ac2/wp-dyn/A5185-2002Jan31.

[2] Robert O'Harrow, "Air Security Focusing on Flier Screening," *Washington Post*, Sept. 4, 2002; online at http://www.washingtonpost.com/ac2/wp-dyn/A34738-2002Sep3.

[3] TSA Press Release, March 11, 2003.

- The same month, consumer activists began an online campaign urging citizens to "Boycott Delta" because the airline was reportedly helping the TSA test CAPPS II. Delta eventually withdrew its co-operation with the government in this area.
- In August 2003, having received fierce criticism for the sweeping nature of its January Federal Register proposal, the TSA issued a new notice attempting (unsuccessfully) to address some of the criticism the agency had received. The new notice expanded the scope of the system to include not just terrorists but also domestic criminals.
- In September 2003, it was revealed that a U.S. carrier, Jet Blue, had "voluntarily" turned over to a contractor working for the government data on 5 million of its customers, sparking a public uproar and several lawsuits against the company.
- Also in September 2003, Congress passed legislation prohibiting CAPPS II from being implemented until the General Accounting Office, the investigative arm of Congress, had certified that the system meet basic criteria of effectiveness and fairness.

2004 - The Fall of CAPPS II and Continuing Legal Challenges

- In January 2004, the TSA announced that, since no airlines would voluntarily hand over their passenger records to the government for the purposes of testing and experimentation with the CAPPS II program, it was planning to compel them to hand over their records.
- Also in January 2004, the TSA said it expected to roll out CAPPS II in the summer of 2004. Government sources, however, told reporters that the system was nowhere near ready.[4]
- Also in January 2004, the Washington Post revealed that Northwest Airlines had shared millions of traveller records with the government to use in "data mining" threat-detection experiments.[5]
- Despite this uncertainty, in April 2004, the European Commission signed an agreement with U.S. allowing for the transfer of Europeans' data to the government – meaning that at a practical level, the private data of Europeans was now more exposed to the U.S. government than that of American citizens, despite the Europeans' purportedly stronger privacy laws.
- In February 2004, the General Accounting Office (GAO) warned that CAPPS II was not sufficiently protecting the privacy of individuals. The GAO found that the TSA failed 7 of the 8 tests set out by Congress for basic effectiveness and respect of privacy, including failures to provide for due process, a minimum level of accuracy, and proper security and oversight. The program was formally barred from going into effect until the GAO certified passage of all those tests.
- In April 2004, the ACLU filed suit over the large number of innocent travellers who had been stopped, questioned, and worse because their names were on a secret government "no-fly" watch list of suspected terrorists, and their continuing inability to get their names removed from that list.
- Also in April, yet another carrier, American Airlines, revealed that it had shared more than a million passenger itineraries with government contractors for the purpose of testing CAPPS II.

[4] Jeremy Tobin, "Passenger Coding System Not Even Close to Ready, Critics Say," *Congressional Quarterly Homeland Security*, Jan. 14, 2004.

[5] Sara Kehaulani Goo, "Northwest Gave U.S. Data on Passengers," *Washington Post*, Jan. 18, 2004; online at http://www.washingtonpost.com/ac2/wp-dyn/A26422-2004Jan17.

- In May 2004, it was discovered that American, United and Northwest Airlines had each turned over millions (up to a year's worth) of customer records to the FBI, which sifted through the data in the hopes of detecting terrorist attacks.[6]
- In July 2004, Homeland Security Secretary Tom Ridge announced that CAPPS II was being dismantled. The acting head of the TSA, David Stone, meanwhile, announced that the TSA was working on "reshaping" the CAPPS II program.
- In August 2004, the TSA announced the launch of a passenger profiling program entitled "Secure Flight." The renamed program was largely a re-branded version of CAPPS II, except that it would not, according to descriptions by TSA officials, use computer algorithms to rate individuals' "threat to aviation," and would not expand its scope beyond terrorism. It did, however, draw on personal information held by private-sector databases, expand the personal information required in making a reservation, utilise secret, unreliable government terrorist watch lists, and lack meaningful due process protections.
- Also in August 2004, Senator Edward M. Kennedy revealed at a committee hearing that he had been stopped and questioned at U.S. airports five times because his name was on a terrorism watch list, and that he had been unable to get removed from the list for more than three weeks despite being a U.S. Senator and brother of a former U.S. president.
- In September 2004, the TSA announced that it would require the airlines to turn over the passenger name records (PNR) details of all their customers who flew during the month of June 2004, to be used for program tests.
- In October 2004, the Secure Flight program director promised that the TSA was going to create a new office where passengers mistakenly labelled as potential terrorists could appeal their cases. The promise came as customers continued to find it difficult or impossible to remove their names from the government's secret "no-fly" and "selectee" terrorist watch lists, despite months and years of complaints and bad publicity.[7]
- Also in October 2004, the president signed the Homeland Security 2005 budget legislation, which contained a provision barring TSA from testing commercial data for Secure Flight until the agency had developed "performance measures" for the test and those measures had been reported upon by the GAO.
- In November 2004, program officials ordered the airlines to turn over customer data, declared that testing of the program would take place that November or December, and that the program would go into operation in "late spring or early summer of 2005."[8]
- In December of 2004, it was reported that the TSA still had not identified either the kind of commercial data it would test or the commercial company that would participate in the test.[9]

2005 - Increasing Doubts and Delays for 'Secure Flight'

- In March 2005, the GAO issued a review of Secure Flight in which it found that TSA had only achieved one of ten Congressional requirements – establishing an internal oversight board – and had not yet even finalised a "draft concept of operations."[10]

[6] John Schwartz and Micheline Maynard, "Airlines Gave F.B.I. Millions of Records on Travelers After 9/11," *New York Times*, May 1, 2004.

[7] Caitlin Harrington, "TSA Promises New Advocacy Office to Clear Errors on No-Fly Lists," *Congressional Quarterly Homeland Security*, Oct. 26, 2004.

[8] Sara Kehaulani Goo, "Airlines Must Hand Over Records", Washington Post, Nov. 13, 2004.

[9] Caitlin Harrinton, "Airline Passenger Screening Plans Still Drawing Jitters," *Congressional Quarterly Homeland Security*, Dec. 3, 2004.

[10] U.S. Government Accountability Office, "Aviation Security, Secure Flight Development and Testing Under Way, but Risks Should be Managed as System is Further Developed," March 28, 2005.

- In June 2005, the DHS's Chief Privacy Officer announced that she was investigating the use of private-sector commercial databases by the Secure Flight program, which the TSA was prohibited from doing without public notice under the Privacy Act's ban on secret databases. In response, the TSA rushed a post-hoc public notice into the Federal Register.[11]
- In July 2005 the GAO issued a report finding that passengers' personal information was used in violation of the federal Privacy Act during testing of Secure Flight in 2004.
- Also in July 2005 the head of Secure Flight said that the government planned to use commercial databases to detect terrorist sleeping cells among airline passengers. This announcement undid the most significant improvement of Secure Flight over CAPPS II, by re-opening the possibility that the government would use secret computer algorithms based on commercial databases and other sources.[12]
- In August 2005, with testing of Secure Flight still not underway, the Department of Justice's Inspector General issued a report saying that DOJ's Terrorist Screening Center (or TSC, which had been created to maintain the U.S. government's watch lists) could not plan to assist in Secure Flight because TSA failed to even establish a working flow chart for Secure Flight.[13] "The TSC does not know when Secure Flight will start, the volume of inquiries expected. . . the quality of data it will have to analyze and the specific details" of how the program would be developed.
- In September 2005, TSA's internal Secure Flight Working Group concluded that "Congress should prohibit live testing of Secure Flight until it receives ... a written statement of the goals of Secure Flight signed by the Secretary of DHS" along with safeguards against abuse and expansion of the program.[14]
- In December 2005, a panel of independent experts advising DHS found that "the program is not yet fully defined."[15]

2006 - Secure Flight Uncertain

- In January 2006, TSA director Kip Hawley stated that it had still not yet been determined precisely how the Secure Flight program would work.[16]
- In February 2006, the GAO issued a report finding that the Secure Flight program appeared to fall short in protecting privacy and system security and was "at serious risk" of failing to be effective because of a failure to rigourously define the program's parameters.[17]
- Later in February 2006, the TSA announced that it was suspending Secure Flight in order to conduct a "comprehensive audit" of the program, due to unnamed security concerns.[18]

[11] See http://www.aclu.org/privacy/spying/15337prs20050616.html, http://www.foxnews.com/story/0,2933,160179,00.html.

[12] Leslie Miller, "U.S. May Use Airline Data to Find Sleepers," Associated Press, July 23, 2005.

[13] "Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program," U.S. Department of Justice Office of the Inspector General, Audit Report 05-34, August 2005, page (ix).

[14] Report of the Secure Flight Working Group, Presented to the TSA, Sept. 19, 2005, at 32.

[15] Department of Homeland Security Data Privacy and Integrity Advisory Committee, "Recommendation on the Secure Flight Program," Adopted Dec. 7, 2005, at 1, 2.

[16] Leslie Miller, "TSA Chief Suspends Traveler Registry Plans," Associated Press, Feb. 9, 2006.

[17] Alice Lipowicz, "GAO: Secure Flight falls short in privacy, system security," *Government Computer News*, Feb. 10, 2006.

[18] Leslie Miller, "TSA Chief Suspends Traveler Registry Plans," Associated Press, Feb. 9, 2006.

- In June 2006, the GAO reported that the TSA had still not completed the steps it had agreed to take as a result of the previous GAO report.[19]
- As of fall 2006, the Secure Flight continues to founder.

Behind the Bureaucratic Failure

Although the story of passenger profiling in the United States is a damning chronicle of failure, it would be a mistake to interpret this series of events as merely a story of bureaucratic indecision and incompetence. Behind the twists and turns in the story lie genuinely knotty problems with the very concept of this kind of system. While it often strikes people as a simple, common-sense matter to "know who is flying, and not let Osama Bin Laden get on a plane," as proponents so often put it, the reality of trying to implement database and background checks in a democratic society is that it introduces many troubling implications and dilemmas, which are a big reason for the programs' failure to launch.

- **Questions about its effectiveness.** Persistent unanswered questions about the actual effectiveness have dogged the program and robbed it of political support. The ACLU and other critics have pointed out that nothing in the system would prevent a terrorist from sailing through it simply by assuming someone else's identity. Unless the system is backed up by a kind of comprehensive cradle-to-grave identity tracking and verification system, it will be plagued with problems. Such a comprehensive system is unpalatable to Americans.
- **Due process and redress.** Despite repeated official claims, decent redress procedures for the airline profiling plans in their various incarnations were never unveiled – and the existing procedures were proven to lie somewhere between useless and non-existent. Checks and balances are vital for this kind of program – but due process would be expensive for the government to administer. And the government has only begun to confront the knotty problems involved in a democratic society when the government tries to build and maintain secret lists and ratings of citizens, and impose what amount to sanctions based on those judgements, without opening up the process in a way that compromises the security value of the program.
- **"Mission creep."** Critics have also pointed out that once put in place, the stage will be set for an inevitable expansion of this program. How will politicians resist expanding it to cover all forms of petty crimes for example? Who will stand up to defend, for example, fathers who fail to pay child support, or whatever other category of petty wrongdoing? How will policy-makers and administrators resist expanding it to new locations, such as bus stops and sports arenas? And what will prevent administrators from drawing upon more and more sources of data in a vain attempt to gather enough information about individuals to make reliable judgements about them?
- **Unreliable watch lists.** Another problem with these programs is that the foundation upon which they are being built – watch lists – is rotten. In the United States, at least, terrorist watch lists have been beset by mismanagement and bloat. Instead of maintaining a narrowly focused list of true terrorists, the lists have been rapidly expanding to alarming size far beyond the number of people that anyone believes are circulating with any intent to attack airliners. The result: innocent people harmed and security resources wasted.

[19] GAO, "Management Challenges Remain for the Transportation Security Administration's Secure Flight Program," June 14, 2006

Conclusions

- No comprehensive identity-based passenger screening system exists in the United States.
- Attempts to create such a program have foundered for several years.
- The attempt to build such a program has failed not only because of government incompetence, but also because the very concept has proven to be far more problematic in a democratic society than it often appears to policy-makers initially.
- Such programs require constant oversight and mandatory reporting in their planning and development stages so that we can ensure that they are being built within legal constraints so that they are consistent with democratic values.
- Europe must tread carefully to avoid these same problems, through generating informed public debate, providing legislative oversight and mandatory reporting, challenging legally the procedures, and questioning the technological and social implications of these designs.