

September 5, 2007

Hugo Teufel III  
Chief Privacy Officer  
Privacy Office, Department of Homeland Security  
Washington, DC 20528

**Re: Comments Regarding the Proposed Automated Targeting System, DHS Docket 2007-0043**

Attention:

The American Civil Liberties Union is writing to formally oppose the continued functioning of the Automated Targeting System-Passenger (“ATS-P”) as described in the Department of Homeland Security Notice of Proposed Rulemaking, 72 C.F.R 43567, dated August 5, 2007. ATS-P is an illegal program which classifies Americans and other travelers entering this county as terrorists based on secret rules and computer analysis. The program violates a clear Congressional mandate and is contrary to good public policy. The Department of Homeland Security (“DHS”) must shut down or severely curtail the operation of ATS-P.

The ACLU is a nationwide, non-partisan organization of more than 500,000 members dedicated to protecting the principles of liberty, freedom, and equality set forth in the Bill of Rights in the United States Constitution. For more than 80 years, the ACLU has sought to preserve and strengthen privacy and equality in American life.

*I. ATS-P Violates Federal Law*

The ATS-P program must be ended or severely curtailed because it is operating in direct violation of federal law. In legislation providing appropriations for DHS for fiscal years 2006, 2007, and 2008, Congress enacted – and twice reiterated – an explicit ban on the use of funds for assigning risk levels to innocent individuals as part of a series of strict privacy controls on passenger prescreening programs. Public Law 109-295, Title V, Sec. 514; Public Law 109-54, Title V, Section 518; Public Law 108-334 Title V, Section 522. With the ATS program, DHS is ignoring that statutory prohibition. Any funding of the ATS-P program by the Department violates each and every one of these appropriation acts.

The 2007 Department of Homeland Security Appropriations Act states in relevant part:

“None of the funds provided in this or previous appropriations Acts may be utilized to develop or test algorithms assigning risk to passengers whose names are not on Government watch lists.” Public Law 109-295, Title V, Sec. 514 (e).<sup>1</sup>

The analysis of violations of the relevant sections of the appropriations acts is a straightforward four-part test: a) Is the funding provided by DHS b) to perform development or testing to create c) an algorithm for assigning risk d) for more than those names on government watch lists. The first part of the test is easily dispensed with. ATS is a system created and controlled by US Customs and Border Protection, a component of the Department of Homeland Security.

ATS was created by the US government as part of another Customs and Border Protection computer system, the Treasury Enforcement Communications System (TECS), so there is no question that its development and testing took place within DHS. 71 Fed. Reg. 64543. Further, according to the original Privacy Impact Assessment performed by DHS:

“A large number of rules are included in the ATS Modules, which encapsulate sophisticated concepts of business activity that help identify suspicious or unusual behavior. The ATS rules are constantly evolving to both meet new threats and refine existing rules.” Privacy Impact Assessment, Customs and Border Protection, Automated Targeting System, November 22, 2006, pg. 3<sup>2</sup>

From this description it is clear that testing and development on the system is ongoing.

There is also little doubt that ATS-P is an algorithm for assigning risk. In the Department’s recently published Privacy Impact Assessment DHS states “ATS-P processes available information from these databases to develop a risk assessment for each traveler. The risk assessment is based on a set of national-and user-defined rules”. PIA, ATS, August 3, 2007, Pg. 5. Testimony before Congress makes this connection even more explicit:

“10. What steps does CBP undertake that passengers and crew are adequately screened at seaport entries? Does CBP coordinate with the Terrorist Screening Center?”

Answer: CBP rigorously screens watch list names from airlines and ships (both crews and passengers), destined to the United States transmitted in advance as mandated by law, through two systems, the Interagency Border Inspection System (IBIS) and Automated Targeting Systems (ATS). IBIS and ATS employ different algorithms to produce potential matches which require additional vetting either prior to or upon arrival.” Testimony before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism and Homeland Security, *DEPARTMENT OF HOMELAND*

---

<sup>1</sup> The language of all three appropriations bills is substantially similar. We have used the most recent version unless otherwise noted.

<sup>2</sup> This same language is repeated in DHS’ 2007 Privacy Impact Assessment. Privacy Impact Assessment, Customs and Border Protection, Automated Targeting System, August 3, 2007, Pg. 4.

*SECURITY LAW ENFORCEMENT EFFORTS AT U.S. PORTS OF ENTRY*,  
March 15, 2005 (response to questions for the record by Commissioner Jayson  
Ahern, U.S. Customs and Border Protection).

All the official descriptions of the program make clear that the entire purpose of ATS-P is to perform risk assessments using algorithms and rule based queries on passengers. ATS assessments are performed on all passengers, not just those on watch lists. According to the PIA, "ATS uses the same risk assessment for everybody." PIA, ATS November 22, 2006, pg. 23. ATS-P processes available information "to develop a risk assessment for each traveler." PIA, ATS November 22, 2006, pg. 4.

Members of Congress share this view of ATS's legality. In a recent hearing on data mining, Senator Patrick Leahy, the Chairman of the Senate Committee on the Judiciary, said the following:

"Just last month Representative Martin Sabo, one of the leaders in enacting legal prohibition developing and testing data mining programs, said to The Washington Post, 'The law clearly prohibits the testing or development of the Department of Homeland Security's ATS data mining program,' even though that's been used for years to secretly assign so-called terrorist scores to law-abiding Americans. I suppose that 90-year-old person in the walker. I will put The Washington Post article as part of the record. All I want is for the administration to follow the law. They want us to follow the law; they ought to follow the law and let us develop what is best. We all want to stop terrorists, but we don't want to make our own government treat us, all of us, like we're terrorists." Senate Committee on the Judiciary, *BALANCING PRIVACY AND SECURITY: THE PRIVACY IMPLICATIONS OF GOVERNMENT DATA MINING PROGRAMS*, January 10, 2007.

In sum, ATS meets all four prongs of the test laid out in the 2007 DHS Appropriations Act and violates a clear Congressional prohibition barring risk assessments systems.

DHS has denied that ATS-P violates the law. According to DHS spokesman Jarrod Agen "[t]he language in the appropriation bill refers specifically to Secure Flight". Ryan Singel, *DHS Passenger Scoring Illegal?* Wired News, December 7, 2006. This reading is, at best, a misinterpretation of the law. Section 514(e) was always meant as a catch all phrase, one that encompassed more than simply Secure Flight. As one of the lead sponsors of the amendment, Representative Martin Sabo, stated "[i]t clearly goes contrary to what we have in law. ATS is the kind of computerized risk assessment we have been trying to prohibit." Michael J. Sniffen, *Traveler Risk System May Violate Ban*, ASSOCIATED PRESS, December 7, 2006.

DHS's contention that the DHS appropriations language applies solely to the Secure Flight program does not comport with either the structure of the relevant legislative sections or plain meaning of Section 514. That section reads:

SEC. 514. (a) None of the funds provided by this or previous appropriations Acts may be obligated for deployment or implementation, on other than a test basis, of the Secure Flight program or any other follow on or successor passenger prescreening program, until the Secretary of Homeland Security certifies, and the Government Accountability Office reports, to the Committees on Appropriations of the Senate and the House of Representatives, that all ten of the conditions contained in paragraphs (1) through (10) of section 522(a) of Public Law 108-334 (118 Stat. 1319) have been successfully met.

(b) The report required by subsection (a) shall be submitted within 90 days after the Secretary provides the requisite certification, and periodically thereafter, if necessary, until the Government Accountability Office confirms that all ten conditions have been successfully met.

(c) Within 90 days of enactment of this Act, the Secretary shall submit to the Committees on Appropriations of the Senate and the House of Representatives a detailed plan that describes: (1) the dates for achieving key milestones, including the date or timeframes that the Secretary will certify the program under subsection (a); and (2) the methodology to be followed to support the Secretary's certification, as required under subsection (a).

(d) During the testing phase permitted by subsection (a), no information gathered from passengers, foreign or domestic air carriers, or reservation systems may be used to screen aviation passengers, or delay or deny boarding to such passengers, except in instances where passenger names are matched to a Government watch list.

(e) None of the funds provided in this or previous appropriations Acts may be utilized to develop or test algorithms assigning risk to passengers whose names are not on Government watch lists.

(f) None of the funds provided in this or previous appropriations Acts may be utilized for data or a database that is obtained from or remains under the control of a non-Federal entity: *Provided*, That this restriction shall not apply to Passenger Name Record data obtained from air carriers. Public Law 109-295, Title V, Sec. 514

A careful reading of the section notes that subsection (a) begins with the language “None of the funds provided by this or previous appropriations Acts” and then describes the criteria necessary to implement the Secure Flight program. Subsections (b) through (d) each then reference back to subsection (a) indicating that they apply to Secure Flight as well. However, with subsection (e), section 514 once again broadens in scope, no longer referring back to subsection (a) and including the “None of the funds provided in this or previous appropriations Acts” language.

Even if the entirety of section 514 was meant to be directed at Secure Flight, this language would still be broad enough to cover ATS-P because this section applies to “Secure Flight program or any other follow on or successor passenger prescreening program.” DHS admits that analysis under ATS-P applies to travelers and “is done in advance of a traveler’s arrival in or departure from the United States.” PIA, ATS, August 3, 2007, pg. 12. In other words ATS-P is clearly a passenger prescreening program.

In short, DHS does not have discretion over continuing the ATS-P program as currently constructed. The Congressional prohibition is explicit. ATS-P is in violation of the law and must be shut down.

## *II. ATS-P Assigns Terrorist Risk Assessments to Everyone Entering or Leaving the Country*

As we discussed above, the purpose of ATS-P is to provide “risk based targeting scenarios and assessments” for travelers into and out of the country. 72 Fed. Reg. 43650 (System of Records Act Notice, ATS, August 6, 2007). DHS repeatedly notes that they are not assigning “a score to determine an individual’s risk level” but instead are “developing a risk assessment for each traveler”. PIA, ATS, August 3, 2007, pg. 11; *Id* at 5. This seems like a distinction without a difference.

Congress continues to reject the rating of the millions of travelers who enter and exit the country every year for a number of very good reasons:

- **Undemocratic ratings.** ATS-P will put the government into the business of creating “security ratings” for millions of its own citizens, an unprecedented step with the potential to alter the relationship between the state and the individual. The United States is a free and open society. As long as individuals obey the law they have the right to live their lives unencumbered by government scrutiny or control. Once the government begins to make important assessments about its citizens outside the bounds of the law they change that dynamic. This creates a system where individual’s movements can be controlled and the considerable powers of the state can be brought to bear on individuals without appropriate oversight or due process.
- **Mission creep.** Once the government goes down this road, mission creep will be inevitable. How much information about a person’s background does the government need in order to truly establish that someone is not a threat to aviation? Because you can’t prove a negative, the government over time will inevitably draw on more and more information, and violate more and more privacy, to generate these ratings. It is also likely that, once established, this ratings system will be used for more and more things – not just travel, but other functions too as other agencies seek to “piggyback” on this ready-established ratings system.
- **Garbage in, garbage out.** This system will likely make judgments based on government databases that we know are already riddled with errors. To take just one example, one of the databases that ATS-P relies on is the National Crime Information Center (NCIC) database. PIA, ATS, August 3, 2007, pg. 31. In 2003 the FBI exempted that system from the Privacy Act. 68 Fed. Reg. 14140. In essence the FBI was admitting that it could not ensure the accuracy and timeliness of incriminating information about a particular individual before loading it into the nation’s most utilized and wide ranging law enforcement database. The

government's refusal to attest to the accuracy of such a critical database raises serious questions about using a secretive database like ATS to make such important judgments about travelers. The result will be a system that will both target innocent individuals, and will be ineffective at targeting many true threats.

- **Questionable effectiveness.** Even aside from the problems created by unreliable source data, it is far from clear that computer algorithms can make good security judgments. The world may be simply too complicated, and individuals' stories and circumstances too varied, for a mindless computer program churning through a defined set of data to make useful judgments. In fact the idea that the government can predict whether an individual will at some future date commit a terrorist act has been at the heart of a number of government efforts to screen passengers including CAPPS II and Secure Flight. None of those efforts were ever implemented. The Secure Flight Working Group, convened by the Transportation Security Administration ("TSA") to provide it with advice on screening issues, concluded that ". . . there is not sufficient available intelligence to determine what characteristics indicate someone will be a threat." Secure Flight Working Group Rep., presented to the TSA, Sept. 19, 2005, at 3.

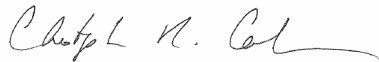
### *III. Conclusion*

Little seems to have changed about the ATS program since its disclosure last November. In spite of broad public outcry, the substance and most of the details of the program remain the same – including its most objectionable elements. The Department of Homeland Security must curb the excesses of ATS and end its continuing and illegal efforts to categorize innocent travelers as security risks based on computer analysis. If DHS is unwilling to act Congress should take further action to end ATS-P and protect the privacy of travelers.

Sincerely,



Barry Steinhardt  
Director, Technology & Liberty Program



Chris Calabrese  
Counsel, Technology & Liberty Program