The Automated Targeting System (ATS)—A Violation of American Law, The EU-US PNR Agreement and Basic Human Rights.

Barry Steinhardt
Director Technology and Liberty Program
American Civil Liberties Union
Bsteinhardt@aclu.org

March 21,2007

Recently, it was revealed that the US government has improperly diverted a tool for screening cargo, the controversial Automated Targeting System (ATS) program, into a data mining program that assigns all who cross the nation's borders, American citizens and foreign visitors-- alike, with a computer-generated "risk assessment" score that will be retained for 40 years.

Many fundamental questions remain unanswered about ATS. The program raises concerns because it brings innocent passengers under government suspicion without justification and it threatens our privacy while undermining our constitutional freedoms and international human rights.

Conflicting statements about a mystery program

The US Government has issued contradictory statements about ATS. For example, Stewart Baker, the Assistant Secretary for Policy at the Department of Homeland Security, claimed in a recent speech that ATS does not involve the scoring of human beings.1 But Baker's assertion is flatly contradicted by other official statements by DHS, including a legally binding Privacy Act "System of Records Notice" (SORN) on this program published in the Federal Register ("ATS builds a risk assessment for cargo, conveyances, and travelers based on criteria and rules developed by CBP"2) as well as an ATS "Privacy Impact Assessment" ("Every traveler and all shipments are processed through ATS, and are subject to a real-time rule based evaluation. ATS provides equitable treatment for all individuals in developing any individual's risk assessment score."3

The need to get real answers

Such contradictions highlight how little the public truly knows about ATS, and reaffirm the need for the US Congress, as well as the European Union and our other allies to thoroughly investigate the program so that it can be publicly debated and the relevant laws enforced. Many fundamental questions remain unanswered about ATS. Is there a risk assessment score? Is it in effect now? Is it retained? If so, how is it used? This subject is too sensitive for policy to be formulated on the ground and in secret by invisible bureaucrats and security agents.

In the US, the American Civil Liberties Union and other human rights group have urged the Congress to examine the powers Homeland Security is claiming for itself for potential future use, without statutory authorization to substantiate that claim. For example, even if the agency is using its discretion not to maintain data for 40 years, as officials have protested is most often the case, the fact remains that the agency has reserved for itself the authority to do just that anytime it pleases.

Vague and misleading claims about the program's successes

DHS officials also advanced broad claims about the purported successes of the ATS program. In Baker's speech, for example, he cited specific anecdotes in which individuals were captured (a man who later carried out a suicide attack in Iraq, a man found with bomb-building literature, and a woman who was later discovered to be working for a human-smuggling program) as a way of dramatizing the program's purported successes.

We can understand why DHS would want to cite these “success stories” to support their program. But since we do not really know exactly what ATS is or how it works, the public has no idea how these successes were achieved, and what role, if any, ATS played in them. More specifically, the public has no ability to judge whether computerized data searches and profile-building (the controversial activities in this program) played a roll in them. Unanswered questions include:

1. Were these catches the result of pure luck? Tens of millions of individuals enter the United States each month, and our customs officers have always turned away some from our borders. Given the millions of

people who cross our borders, people are turned away for many reasons in the course of regular business. For example, their papers may not be in order. Yet, these people may have no connection to terror or crime. If Customs and Border Protection ("CBP") were using psychics or palm-readers to pick travelers for further scrutiny, pure chance would still guarantee the agency some success stories it could point to in a speech. But such isolated cases tell us nothing about whether this system is truly effective.

2. Does the government even know whether the system is effective? Baker makes no mention of any systematic audit or other evaluation by the government to determine whether this program is more effective than blind chance, and enough so to justify its costs. For example, it is unknown whether the government simply assumes that every person turned away represents a success - that such persons were in fact guilty of whatever suspicion led to their rejection.

3. Were these catches the result of old-fashioned sleuthing? In one purported success cited by Baker, an individual was denied entry based upon an interview by a customs officer, and the fact that he could not withstand such in-person human scrutiny. Such interviews long predated the invention of computerized "risk assessments," and Baker provides no reason to believe that computer risk scores contributed at all to the decision not to admit him. In another anecdote, Baker claims that ATS allowed agents to take down an international human-smuggling ring. But the destruction of that ring was a result of old-fashioned, predicate-based investigation, and in no way justifies the collection and maintenance of data on millions of Americans and the construction of computer-generated "threat scores" on them, a controversial activity in this program.

4. Were these catches the result of simple watch list checks? Watch lists are a primary part of ATS, and Baker says simply that "data in the DHS computer system flagged" these individuals. If watch list comparisons led to Baker's claimed "successes," then programs other than ATS deserve the credit and ATS risk score assessment of innocent travelers remains unjustified.

A dangerous road to follow

Although government spokespersons strain mightily to portray ATS as a harmless, commonsense system, it is just the kind of data mining approach to terrorism that raises very serious and fundamental questions about privacy.

* "Limited information" claims are misleading. Government defenders of ATS talk about its use of "limited information." But just what are the limits on the information being used here? It its Federal Register notice, DHS set no limits on the kinds of "individualized information" that could be used to form these judgments - and indeed, granted to itself sweeping exemptions to the Privacy Act, which was passed partly to stop just this kind of dragnet approach to law enforcement.

* Legal standard, not current practice is the issue. DHS officials are straining to emphasize that ATS contains harmless data and poses no threat to privacy. To begin with, DHS's evasion of its public notice requirement leaves the public without any basis to evaluate such claims given the program's secrecy. Furthermore, officials may well proclaim in a speech that the security agencies are, at the moment and for the time being, only using limited information. But with the legally binding definition of this program that has actually been put into writing in the Federal Register, the government is attempting to legally establish for itself the authority to build something considerably more sweeping. Even if today CBP's statements are factually correct, DHS clearly has far grander plans for the privacy-invasive information they are now routinely collecting.

Current limits are not likely to stand

There is, in fact, every reason to believe that this program will become more sweeping. Just how much information about a person's background does the government need in order to truly establish that someone is not a threat in any way?

There are no obvious natural limits to the data in which the government might find "patterns that establish reason to ask questions," as Baker put it. Does the government get to scrutinize every address at which you've ever lived? Quiz you about the fact that you once went for 12 months without a

job? About your Web surfing, your online book purchases, your school transcripts, your internal movements, your associations, your ex-spouse?

That is all data that could be conceivably be "relevant" to an attempt to detect a terrorist threat, or criminal wrongdoing. That is all data that could become part of the ATS system within the "limits" defined by the notice published in the Federal Register. If the government really intends to use information only in much more limited ways, then such limits should be enacted into hard law.

Because you can't prove a negative, it is entirely predictable and indeed inevitable that over time, if not checked by an insistence on our collective values of privacy, the government will push for more and more sources of information out of which to build these ratings.

To the question of how much data the government should have access to, the implicit answer given by ATS's defenders is "as much as it needs." But that "need," will prove bottomless unless it is counterbalanced by our ideals of privacy and limited government - balancing values that are missing from the design of this program. Perhaps it is too much to expect that those who work in our security agencies can themselves keep in perspective those larger counterbalancing civic ideals.

Questionable Legality

ATS appears to be in violation of both American Law and the PNR agreement between the US and the European Union.

The US Congress has already acted several times to prohibit this sort of invasive passenger profiling, having included an explicit ban on the risk scoring of innocent individuals in the Homeland Security appropriations bills for 2005, 2006 and 2007. However, with the ATS program, DHS directly ignored that statutory prohibition. The agency's disrespect for clear statutory law and congressional intention cannot go unnoticed

Of particular relevance to the European Parliament the scheme directly contravenes the EU-US agreement on the transfer of passenger data.

The DHS has exempted ATS from the 1974 Privacy Act by preventing individuals from exercising any right of access to this profile and any right

to modify or correct information. According to the Privacy Impact Assessment published by DHS, "There is no procedure to correct the risk assessment and associated rules stored in ATS." This directly contravenes the EU-US agreement, which specified a number of actionable rights for Europeans to appeal against the misuse and abuse of their personal data. CBP and DHS may use this profile for any number of purposes. According to the DHS, the driving purpose behind ATS is "to perform targeting of individuals, including passengers and crew, focusing CBP resources by identifying persons who may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law." It may also be used "to assist in the enforcement of the laws enforced or administered by DHS, including those related to counterterrorism." This directly contravenes the EU-US agreement, which limited the use of PNR to combating terrorism and serious trans-national crime.

During the drafting of the original agreement a great amount of concern was expressed regarding the use of PNR for the purpose of profiling and data mining. According to the Article 29 Working Party, passenger risk-assessment systems, such as the now-defunct Computer Assisted Passenger Pre-Screening System (CAPPS II), should never be applied:

"In fact, these [risk-assessment] systems are qualitatively different from the mere transfer of passenger PNR data and involve wide-ranging issues which should be clarified and specifically addressed by the Working Party, in consideration of the more pervasive effects that would affect the fundamental rights of the data subjects concerned. In particular, the CAPPS II system raises a number of peculiar issues that require not only specific consideration by the Working Party, but also different, higher safeguards.

Instead of gaining stronger safeguards, Europe now faces a situation where the PNR agreement has been fundamentally undermined by this additional processing by the Department of Homeland Security.