

Improving On the Current “Watch List” Approach

There are many horror stories relative to false matches to the “no fly” watch list. The common “knee jerk” reaction is to blame the TSA, the TSA screeners, or the airline clerk. This is understandable and in some cases warranted. I doubt that any screener has personally bought on the concept of “wandering” a 2-8 year old (Note: This is not TSA policy, rather, it is a violation of their publicly stated position.) Screeners often are not trained to think, only to follow guidelines; guidelines that often have a strong smell of CYA. The thought process is that, because there is a possibility that a child, senior citizen, or physically handicapped individual may be a carrier of contraband materials, then they must be treated like everyone else. Many people will be offended and their will be many holes left in security by any system that relies on random screening and name matching. The system is doomed if the rules are rigid and penalties are in place for failure to comply with guidelines. A better criterion is needed for selecting those who will be looked at closer.

In a broad range of situations, interrogation prior to the pat down and the right to use personal judgment to act upon the assessment of the risk will quickly allow determination of there is a need to proceed further. In the case of children, elderly, or handicapped potentially being couriers; bribery, blackmail, fanaticism and physical intimidation are the reasons why they would be involved in such a criminal act. Answers to a well established set of questions and the behavior of the individual as they respond to them will quickly establish whether there is a need to proceed with more in depth screening. This is one component in behavior profiling.

There was an attempt (CAPPS II) made several years ago to collect passenger data to develop a behavioral model with the intent to use the model to develop a usable profile for distinguishing the “good” guys from the possible “bad” guys. The purpose was to pre-screen passenger lists and to allocate limited resources, primarily, to those with a behavior pattern (profile) that suggested some potential for criminal activity. This was scrapped due to an outcry by privacy advocates and the unfounded claims by the uninformed that it wouldn't work. I say unfounded because only implementation of at least a “pilot” program could actually measure the various parameters necessary to assess its effectiveness versus cost and invasion of privacy. The program has since been “reinvented” as [Secure Flight](#). I believe that critical elements of what is discussed below have been incorporated into the program. However, certain key elements appear to be missing.

Privacy and security are based on the same principle of sharing information only on a “need to know” basis. It is well understood that trying to intercept terrorists at the point of attack is necessary; but, it has a high risk of failure and, hence, increases danger to the public and infrastructure. The process by itself increases the “fear factor.” There is a better chance of providing protection and reducing fear by using collection and dissemination of intelligence information to thwart

attempts to do harm while they are still in the planning and preparation stages. Evaluation of traveler risk well before or as the journey begins provides the best chance of success and the best protection of privacy (if done out of the public eye).

Impartial automated computer pre-screening can be done without disruption to the passengers or exposure to embarrassing, unwarranted public attention. There is no need for the screener/interrogator to know any personal data regarding the individual and random screening (with some categories of people excluded) will mask any false perception of racial, religious, age, or ethnic profiling. Public profiling based on biographic factors alone does not work and subjects large numbers of people to unnecessary attention. This results in great inefficiency and takes resources away from closer scrutiny of those whose behavior suggests that they are a potential risk. There needs to be a base level of screening for truly hazardous materials that have no legitimate need to be carried on an aircraft, but it does not need to be burdensome.

There are some basic things that can be done to avoid the horror stories. A simple name-based “watch list” will never work well. Truly bad guys likely will not operate under their real identity and banning them from boarding based on a name check without any law enforcement action at the point of contact only serves to alert them that they are being watched. This can cause a confrontation with an ill-equipped person in a public arena. Only a fraction of the names on the “no fly” list are people whom the airlines have designated as “disruptive.” Most names on the list do not have their origin with the TSA. DHS, FBI, foreign governments, and various intelligence agencies are the major contributors. A large percentage of people on the list were placed there without a disciplined process checking why they should be put there. The two step process of a “watch list” (550,000) escalated to a “no fly” list (50,000) is a must, if there is no model being applied to filter out the “noise” and immediately add high-risk individuals to the “no fly” list. Otherwise, with 500,000 names on the list, most of us would be subjected to the horror story.

A name without any biographic or demographic cross checks drowns in a huge sea of miss-spelled, similar, and similar sounding counterparts. Obviously it is beyond allowable time constraints for an airline clerk or TSA screener to cross check and make a judgment based on such parameters. This information would be exposed to many people who have no real need to know and the conclusions would be conditioned by all the human frailties that jeopardize accuracy and consistency.

The short answer is automation. As a part of the travel booking collect the name, issuer, and document number on the identity document that is to be used for the trip or a surrogate to be specified for the underage. It would also be useful to ask for a handicapped indicator. Issuers can be queried through a Trust Authority as to the correctness of the provided document information. For instances where there is a potential “watch list” match, then any supplemental data such as birth

date range, sex, address (all or part), etc. available for the suspect individual would be merged with the document query. No information is returned to the query other than the degree to which there was a match on each data field. This is a major provision to protect privacy by not sharing any data that is not already known.

At security check in the document can be automatically authenticated and cross-checked to match the presented document to the one specified at booking and the boarding pass. The photo can be magnified for easier comparison to the traveler by the inspector. The technology exists. The time is comparable to the manual process used to day and it would be many times more reliable. The inspector can glance at the document for tampering and observe the behavior of the traveler during the 5-10 seconds that the entire process would take. The “hits” that indicate enhanced interrogation (the next step in behavior-based profiling) and possibly more extensive searches would be referred to a separate isolated line with pre-alerted law enforcement observers. Any confrontation should take place in a manner and location that does not jeopardize by standers; hence, it should not be initiated by an airline clerk. Randomly a sampling of passengers who do not alert the system (preconditioned by age derived from the travel document and the handicapped designator captured at time of booking) would be included in the referral to the special screening line. This added truly random element would remove the stigma from under going the extra scrutiny and not prematurely alert a possible criminal/terrorist.

Automation also adds the benefit of a self-auditing process that measures performance of each phase. It provides the opportunity to evaluate overall effectiveness and individual performance of people and equipment.

The boarding pass issued to likely “watch list” match passengers could be coded in such a manner that boarding would only be allowed upon being cleared by the enhanced screening process. Also, swapping of boarding passes could be an issue in some environments. In that case there would need to be a further biometric (facial, finger, iris,...) validation prior to boarding at the gate.

Behind the scenes cross relationships amongst passengers and travel patterns can be automatically evaluated and tracked by document type and number without any privacy invasion. Behavior models derived from this information would be very useful in focusing intelligence resources on likely sources of criminal threats. If combined with records of HAZMAT purchases and other important purchase, communications, or transportation information a set of patterns would emerge that would provide a very good real-time indication that there is probable cause to seek authority to conduct invasive investigations of suspect(s).

There are many details that would need to be resolved and stakeholders that would need to buy-in. This is only a skeleton of what a solution might be.