

Greg M. Bednarski
Technical Analysis 1: **CAPPS II**
February 8th, 2004

With our growing use and dependence on large-scale database systems to manage everything from financial records to transport passenger lists, we're beginning to experience significant information overload. In the realm of airline passenger lists, specifically, our law enforcement and transportation safety agencies are having great difficulty identifying known and potential terrorists who may attempt to injure airline passengers, re-create a September 11th scenario, or worse. To overcome this library-without-a-librarian issue, the Total Information Awareness project (later known as Terrorist Information Awareness) was created to develop data mining technology used to draw correlations from multiple databases, both public and private, to highlight potential criminals based on spending habits, locales, known associations, etc. This project was eventually denied funding over concerns of privacy invasion against US citizens, but the need to protect our commercial airlines still exists. To that end, the CAPPS II system (Computer Assisted Passenger Prescreening System) is being developed to identify potential high-risk passengers using similar data mining technology as the now defunct TIA project. But, we have to ask, does this also generate 4th Amendment concerns? Can it accomplish its mission?

According to the TSA, CAPPS II will authenticate the identity of passengers by checking the passenger name record - including full name, home address, telephone number and date of birth - against commercial databases (*editorial*: would Osama Bin Laden check in under "Bin Laden, Osama"?). In addition, a risk assessment will be done by checking passenger names against government databases, and discarding the information within a few days for "the vast majority of passengers". Admiral James M. Loy, the administrator of the TSA, has stated "We will accomplish this without compromising the privacy and civil liberties enjoyed by every American". How? The TSA contends the information gathered will be no more than what airlines currently gather from all customers, and the databases accessed to calculate threat scores are the same that are used every day by commercial and private enterprises. Finally, the TSA will never see the data used to generate these scores, only the green/yellow/red score indicating a threat level of a particular individual.

As expected, a large variety of civil liberty groups are opposing the CAPPS II project, including the Electronic Frontier Foundation and ACLU. Their concerns run from the commonly expected (what *e/se* will this data be used for?) to the extreme (the ACLU goes as far as calling it un-American and states it will make every American a 'suspect'). Political rhetoric aside, there are some valid concerns I see with a system such as this. Mainly, quality and integrity of the data used to generate scores, correction of inaccurate data, and potential abuse of the information collected.

Regarding quality of data, we need to look at the sources. Although the listing of data sources has not been made public, we can assume databases of a specific nature will be required: airline records, criminal records, terrorist watch lists, credit and/or spending records. Credit and spending reports can't be guaranteed for accuracy – how often does identity theft occur? If someone purchased a one-way flight to Libya last month on your stolen credit card number, would you get flagged? On the whole, commercial databases have a very high standard of data quality, but in regards to governmental databases, according to Steve McCraw, Assistant Director of the Office of Intelligence at the FBI, the National Crimes Information Center (NCIC) database is not required to meet the same standard for accuracy as other public sector databases. If this source were to be used, what would the implications be?

The flip-side of this concern asks: what opportunity does the public have to access data collected on them, and correct if inaccurate? The process involved in redressing your own records after becoming the victim of identity theft can take almost three months. An unfortunate situation like this should not limit one's ability to travel on commercial airlines, so a specific and expedient process must be created to correct records.

As to the integrity of data, valid concern exists over the security of the data collected. We all know 'secure' systems are never 100% impervious to compromise – how far would a dedicated group (perhaps a foreign intelligence organization?) go to acquire any stored data? This may never be known.

Finally, mission creep is always a concern when dealing with somewhat clandestine information-gathering projects. The details of the project, understandably, cannot be enumerated to the general public due to security concerns, but at the same time this places the TSA in the near impossible position of allaying our privacy fears. The nature of the project makes transparency a difficulty, and simply telling the public to "trust us" does not bode well for the future of the project.

With all this being said, one fact remains: we *need* an automated and accurate method to quickly scour our vast ocean of data in an effort to protect those using our airlines. The CAPPS II technology would provide this answer, but specific assurances (privacy, integrity, and accuracy) must be made to the American public before it sees the light of day.