URL: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13356&c=206

The Five Problems With CAPPS II
August 25, 2003

The new version of CAPPS II is all dressed up in the language of privacy and concern for freedom, but it fails to address the core problems with the concept, and continues to pose an enormous threat to American freedom and privacy.

The Five Problems With CAPPS II: Why the Airline Passenger Profiling Proposal Should Be Abandoned

Background

The Transportation Security Agency recently issued a new description of its Computer Assisted Passenger Pre-screening System II (CAPPS II) program, a frightening system designed to perform background checks on the 100 million Americans who fly each year to determine their "risk" to airline safety. TSA received fierce criticism for the sweeping nature of its first proposal, which was published in the Federal Register in January 2003 as required by the Privacy Act of 1974. As a result, TSA on August 1, 2003 issued a new notice, informing the public of its intent to begin testing the CAPPS II program and attempting to address some of the criticism the agency had received.

They failed. The new version of CAPPS II is all dressed up in the language of privacy and concern for freedom, but it fails to address the core problems with the concept, and continues to pose an enormous threat to American freedom and privacy. It will make us neither safe or free.

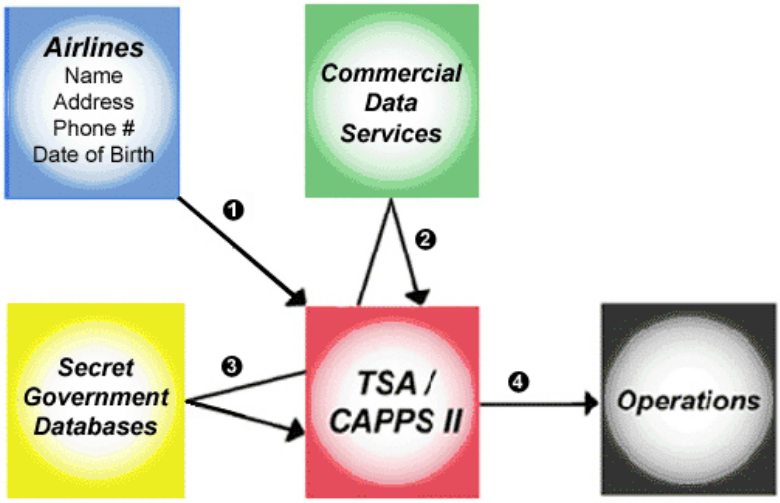
How CAPPS II Works

According to the TSA's notice, CAPPS II will proceed through four steps:

> **1. Collection of 4 pieces of information.** The passenger reservation system will have to be rebuilt to allow the airlines to collect from every passenger, and pass along to the TSA, four pieces of information: name, address, phone number, and date of birth (DOB). With the sometimes exception of the passenger's full name, this information is not routinely collected. (The airlines may also pass along other information that is part of individuals' travel records, some of it potentially sensitive.)
>
> **2. Authentication check.** TSA will send those four pieces of information to commercial data services – data aggregators – which are companies in the business of compiling extensive dossiers about the lives of most Americans. The commercial data services will return back to the TSA an "authentication score" intended to indicate "a confidence level in that passenger's identity."
>
> We simply don't know what will happen to the many Americans, who because of their age, low income, or other factors do not have sufficient records to have their identities verified.

3. Risk assessment score. TSA will run the passenger through a "risk assessment function" that involves unknown secret law enforcement, intelligence, or other government databases. TSA has not released details about this step and does not intend to. As a result of this process – based on both secret data and secret criteria for evaluating that data – each passenger will be given a score measuring their "risk" to passenger or aviation security. Each person will be scored as either "high," "low," or "unknown" risk.

4. Action at the airport. Each passenger's risk score will then be forwarded to security personnel at the airport. Law enforcement authorities would be notified if passengers receive a "high" risk assessment. Those who score "unknown" would be subjected to heightened scrutiny and those who have a "low" score would pass through the ordinary airport screening process.



The Five Biggest Problems with CAPPS II

CAPPS II poses a huge threat to Americans' privacy, and must be stopped. Questions about this new passenger profiling system abound, but its five biggest problems are:

1. The Black Box: Americans Judged In Secret

The biggest problem with CAPPS II is that, simply put, we have no idea what it will do. Once the TSA has obtained your four pieces of information, and run them by the commercial data service, it then generates your "risk score." That score will be based on information from unknown sources that will include shadowy intelligence and law enforcement databases and any other data sources that the TSA decides it would like to collect about you. TSA personnel have issued public assurances that the system will not rely upon medical or financial data, but when it comes to what's in writing – the Privacy Act notice – the TSA specifically exempts itself from having to publish the "sources of records" upon which the system will draw. That means that even if they don't use credit scores today, they could reverse that decision at any time – going back to their original plans – without telling the public.

In short, CAPPS II would involve the construction of an unprecedented infrastructure for conducting background checks on Americans when they fly, and making judgments about how "risky" each of us are – all in secret. CAPPS II would use information sources that are never disclosed to fliers or the public, or subject to public oversight and control, and analyze that information using criteria that are also never disclosed or subject to public oversight.

2. Effectiveness: This System Will Not Make Us Any Safer

Why build CAPPS II if it won't make us any safer?

Even a known, wanted terrorist could sail right through this system simply by committing identity theft (which as we all know is all too easy today) and obtaining a false driver's license or passport (which is even easier). For example, such a terrorist might present a driver's license with their own photograph, but the name, address, phone number and DOB of an innocent person (data that for most Americans can be purchased online for about $50). Nothing in the CAPPS II program would stop such a terrorist. This system is like a Maginot line – the heavily fortified defensive frontier constructed by the French before World War II, which was rendered useless when Hitler's army simply went around it.

And even a tiny error rate would create huge problems. Each year, 100 million Americans fly, many of us more than once. Total passenger transactions each year have been estimated to be as high as one billion. CAPPS II would check every one of those transactions. Even if we assume an unrealistic accuracy rate of 99.9%, mistakes will be made on approximately one million transactions, and 100,000 separate individuals. Those mistakes will result in not only a lot of innocent people coming under suspicion – or worse – but will make it extremely hard to find the handful of real terrorists amid the ocean of false positives.

The error rate will likely be worsened if TSA carries out their announced plan to begin checking passengers for outstanding criminal warrants. The source for that information will most likely be the FBI's giant criminal database known as NCIC (for National Crime Information Center). Normally, the law would require that such a database be maintained with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness" to individuals affected by it. Unfortunately, however, the accuracy of the information in the NCIC is apparently so poor that the Justice Department in April 2003 specifically exempted the NCIC from the accuracy requirement. And yet this same database would become the basis for stopping and harassing thousands of Americans – and diverting limited security resources.

While these shortcomings are being ignored now, once this system is sold to the American people, they will inevitably be used to justify demands for an airtight, cradle-to-grave, biometric national identity and tracking system that would change what it means to live in America (but in all likelihood still fail to thwart terrorism).

3. Mission Creep: Build It And It Will Grow

In addition, once this system is sold to the American people, it will inevitably be expanded – and in more ways than one:

- **The data it draws upon.** We don't know what sources of information the program will plug into; it could be just a few terrorist watch lists to start with. But inevitably, over time the government will seek to add more and more data sources to its background checks in a never-ending attempt to detect terrorists. The CAPPS II Privacy Act notice says that the system will draw upon not only watch lists but also "other information pertinent to the detection of terrorists." That broad language would permit the addition of all manner of new data sources into the program. And again, there would be no public notification or oversight over those sources. In short order the system could become something identical to the Pentagon's "Total Information Awareness" concept, a true Big Brother proposal to monitor all available data sources about us in order to search for suspicious patterns of activity.
- **The purposes for which it is used.** Only a few months ago TSA officials were issuing public assurances that CAPPS II would remain confined to searching for foreign terrorists. Now it has been expanded to include domestic terrorists and violent criminals – all before the program is even officially launched. And the definition of "domestic terrorist" is being steadily expanded far beyond the everyday meaning, potentially encompassing political protesters and – if recent proposals are accepted – even suspects in the "war on drugs." And how long before the system is expanded to search for con-artists, drug dealers, deadbeat dads, and so on down the scale of wrongdoing until it becomes a comprehensive net for enforcing even the most obscure rules and regulations?
- **The places where it is deployed.** TSA director Admiral James Loy has explicitly indicated that the agency envisions expansion of CAPPS II beyond airports to other transportation hubs such as ports. Train stations, bus stations, secure office buildings, concerts – where will it end? Airports today, a totalitarian system of internal government checkpoints tomorrow.

4. Due Process: No Notification, No Correction, No Appeal

Because the core security evaluations at the heart of CAPPS II are completely secret, individuals singled out by the program will have no way of knowing why they have been targeted. They will not know if they are the victim of the widespread inaccuracies that riddle government and private databases, and will have no way to correct such errors if they are. They will have no way of knowing if they have been falsely accused of wrongdoing by someone, or have been discriminated against because of their religion, race, ethnic origin, or political beliefs.

The CAPPS II Privacy Act notice includes a procedure for passengers to access their records, and to "contest or seek amendment of" those records. That procedure is largely meaningless, however. It would only apply to the non-secret part of CAPPS, the information passed along to the TSA by the airlines. In any case the Privacy Act notice says that that data will be deleted "within a set number of days" after travel. That is misleading because the information that will be of true concern to travelers – the data used to assign Americans their "risk scores" – will not be available for review or correction. Once again we are being told "trust us, we're the government. We will correct our own mistakes."

The Kafkaesque potential of this system has been starkly demonstrated by the government's existing "no-fly" lists, under which many innocent, law abiding Americans have found themselves subject to relentless hassles, interrogation and searches every time they try to travel by air – and have been unable to clear their names in the federal bureaucracy. CAPPS II will be an even more intrusive form of data mining that, like the no-fly list, will rely on both secret and inevitably incorrect information to make accusations against individuals.

5. Discriminatory impact: the potential for systematic unequal treatment

While CAPPS II remains shrouded in mystery and its details hidden in black boxes, there is a very real possibility that it will treat Americans unequally based on characteristics such as race, religion, and ethnic origin. CAPPS II will rely on both commercial and government databases, both of which there is ample reason to suspect contain biases against particular groups. For example, credit scores – judgments about individual reliability made by a handful of private corporations – are notoriously sloppy, and on average minority populations have lower scores and are more likely to have no credit record. And it is likely that government security databases discriminate against ethnic and religious groups such as Arabs and Muslims. The points where the system is open to discriminatory impact include:

- **The commercial databases.** While the CAPPS II "authentication check" would rely on commercial data services for nothing more than checking name, address, phone number, and DOB, it is possible that the data services possess this data for a fewer proportion of minorities than they do for non-minorities, or contain more inaccuracies for such individuals. This could be true because, for example, African-Americans and Hispanics tend to move more often than non-Hispanic whites, and would therefore be more likely to find that the information held about them by the data services is out of date.
- **The black box.** The secret risk-scoring portion of the CAPPS II process could include any number of data sources that have a discriminatory impact on the process. For example, although TSA officials have denied any intention of drawing on credit scores, which have a well-documented bias against minorities, nothing in the Privacy Act notice bars the government from doing so as part of the secret risk assessment process.

The bottom line is that we just don't have enough information about this program to allay well-founded suspicions that its burden would not be shared by all Americans equally. And it contains absolutely no mechanism for taking measurements to make sure that such discriminatory impacts do not emerge.

Take Action on this issue at:
http://www.aclu.org/Privacy/Privacy.cfm?ID=13332&c=39