Los Angeles Times

Los Angeles Times

October 2, 2003

The Nation
COLUMN ONE
A Suspect Computer Program
The government is working to better screen airline travelers.But human motivation can frustrate even the most elaborate systems.

Author: Charles Piller and Ricardo Alonso-Zaldivar; Times Staff Writers
National Desk

Edition: Home Edition
Section: Main News
Page: A-1

Index Terms:
TECHNOLOGY
SECURITY
TERRORISM
UNITED STATES
COMPUTER ASSISTED PASSENGER PRE-SCREENING SYSTEM
PRIVACY
AIRPORT SECURITY
Non dup
Infographic

Estimated printed pages: 8

Article Text:

A secret computer program detected something suspicious about the middle-aged passenger heading to Eugene, Ore.

He traveled often, usually taking one-way flights on short notice. In the months following the Sept. 11 attacks, every time he tried to board a flight in Portland, he was pulled out of line and searched as a possible terrorist threat.

The passenger was Peter A. DeFazio -- congressman from Oregon, former Air Force officer and ranking Democrat on the House subcommittee overseeing airline security.

"My constituents found it very amusing," DeFazio said.

It soon became less humorous when he learned he could stop triggering the security checks by simply

joining a frequent flier program, a trick that in the computer's mind transformed him from a suspect into a trusted customer.

"A terrorist can't figure that out?" DeFazio asked.

Since the Sept. 11 attacks, creating an effective system to screen out both known terrorists and would-be hijackers -- plotters with spotless records but nefarious intent -- from millions of airline passengers has become a top priority in the war against terrorism.

But as DeFazio's experience showed, even the most elaborate current computer systems stumble when trying to decipher human motivations, and, like any security scheme, have been perpetually vulnerable to being gamed.

In the face of such challenges, the federal government has embarked on a costly program to create a second-generation profiling system designed to verify the identity of every passenger and analyze their lives through a "black box" of government intelligence and law enforcement databases. Though details of the system are secret, security experts believe that more than 100 factors will be used to sniff out terrorists based on telephone records, travel patterns, law enforcement files and other sources.

The system will turn the new federal Transportation Security Administration into one of the most intrusive government agencies, perhaps second only to the Internal Revenue Service -- investigating about 70 million passengers who take 675 million trips by air annually.

And possibly, all for an illusion of security.

"The U.S. is so much oriented toward a technology [solution] that the people are serving the technology," said Offer Einav, former director of security for Israel's national airline, El Al, widely considered the world's most secure carrier. Like other aviation security experts, he views computer profiling as beneficial only if paired with seasoned security officials who exercise common sense and conduct their own psychological assessments of passengers -- not part of the U.S. program.

"They are dealing with enemies who are human beings. Human beings will always beat the technology," Einav said.

Mixed Success

No computer-based system has ever verifiably thwarted a hijacking or bombing, according to federal and private security experts. But given the enormousness of the task, the airline industry's current system -- the Computer Assisted Passenger Pre-Screening system, or CAPPS -- has occasionally shown flashes of brilliance.

Its greatest success may have been on Sept. 11, 2001. In the 24 hours leading up to the hijackings, CAPPS would have checked more than 1.8 million passengers. It actually flagged six of the 19 terrorists later involved in the hijackings, according to the national commission on the Sept. 11 attacks. About 92,000 innocent travelers were also singled out.

Unfortunately, only a brief luggage check for explosives and weapons was required. The hijackers -- and the then-legal box cutters several were carrying -- were all welcomed aboard their flights.

CAPPS was deployed in 1998, following the crash of TWA Flight 800 off Long Island two years earlier.

It was part of a package of anti-terrorism measures put in place -- including baggage X-rays and bomb-sniffing dogs -- even though mechanical failure was later blamed for the crash.

The system largely relies on government watch lists and passenger travel histories. It provides a relatively rudimentary check that the industry designed as a compromise between maintaining efficiency in boarding passengers and finding possible terrorists, said consultant Douglas Laird, former security director for Northwest Airlines, who helped develop CAPPS.

Laird praised CAPPS for targeting nearly a third of the Sept. 11 hijackers. "What failed on 9/11 was the follow-up," he said.

After the events of Sept. 11 exposed CAPPS' weaknesses, the airlines and the government tried to compensate by hedging their bets -- flagging 15% to 20% of travelers -- an estimated 370,000 per day -- for hand luggage searches and extra security checks. That is an increase from 5% in 2001, according to the TSA.

But casting such a wide net can overwhelm the system, resulting in long delays at the airport. The government believes the best way to increase security and efficiency is to create a more advanced computer system.

CAPPS II, an upgrade expected to cost more than $105 million, is designed to transform a few simple database searches into an omniscient eye on terrorism. The TSA, which will operate the system, plans to introduce it next year. "I don't think there is a single project that will do more potential good for aviation security," said Adm. James M. Loy, head of the TSA. CAPPS II will have "an astonishing capability" to trace would-be terrorists, even if they lead apparently unremarkable lives, he added.

In addition to checking travel records, CAPPS II would require each passenger to provide his name, birth date, home address and phone number when making a reservation. Commercial database companies would check the information against billions of public records and issue an identity rating, handicapping the likelihood that the passenger is lying and judging how "rooted" the person is in a community, rating such factors as local family connections and the amount of time in the same home.

The government would then check the information against national security and law enforcement watch lists of more than 100,000 suspects. It would mine CIA, FBI and other intelligence databases to pluck the rare unknown terrorist from an ocean of innocents with a kind of technological mind-reading.

The government estimates that no more than 4% of passengers -- about 74,000 people a day -- would be rated "unknown risk/yellow light" by CAPPS II and get closer screening, such as shoe checks and physical searches of carry-on items.

An average of only one or two people per day would be rated "high risk/red light" and be barred from flying or even arrested.

Those are the theoretical projections. Reality could be far different.

"Systems that involve wholesale surveillance of innocents tend not to work," said Bruce Schneier, a leading cryptographer and chief technical officer of Counterpane Internet Security, a cyber-security firm. "It's not feasible to catch the bad guys without also catching too many good guys."

Innocent Victim

Consider the experience of Joe Adams of Cottage Grove, Minn., an unassuming, 71-year-old scholar of British literature, who travels for pleasure and his part-time job grading college entrance exams.

Adams was flagged by CAPPS more than a dozen times between April 2002 and this August. At first he was perplexed, then frustrated and finally angered at being treated like a national security threat for up to two hours every time he flew.

Adams eventually learned the reason: His name, like hundreds of other Joe Adamses nationwide, resembled an alias of an alleged Al Qaeda operative.

"I appreciate what they are trying to do security-wise," Adams said. "What I don't appreciate is what they are trying to do to someone like me," someone improbably old for such a mission. "I could be [a terrorist's] grandpa."

Adams' problem eventually disappeared without explanation. Many others simply put up with such treatment. Calls to seven random Joseph Adamses around the country turned up five who fly regularly and share the literature scholar's plight.

One Massachusetts grandmother of 12, whose husband is named Joseph Adams, was told by an airport screener that she was flagged as not just a regular security risk, but a high security risk.

By design, computer profiling systems flag millions of people for such common reasons as moving often, visiting the Middle East or being unlucky enough to share a name with someone on the watch list. The result is an enormous error rate that can overwhelm screeners.

At the same time, the systems are necessarily blinded from considering some factors. For example, ethnic, religious or racial designations are excluded from today's CAPPS and CAPPS II to avoid discrimination.

Linking those factors to terrorism may be an application of crude stereotypes, but from a security standpoint, barring such identifiers doesn't make sense, Einav said.

"As far as I remember, none of the Al Qaeda members was a citizen of the state of Switzerland or was a Catholic priest," Einav said. "Unfortunately, cells of Al Qaeda are existing in Islamic states."

The Sept. 11 terrorists understood that a successful hijacking depended on exploiting precisely these types of holes in the computer profiling system.

In the months leading up to the attacks, they tried several dry runs to see if their efforts to remain invisible to the security system had paid off, according to the joint House-Senate intelligence report on the attacks, issued last December.

"Transparency is the Achilles' heel" of CAPPS, letting attackers "reverse engineer" the system, wrote Samidh Chakrabarti and Aaron Strauss, students from the Massachusetts Institute of Technology and Harvard University, whose computer science class paper raised eyebrows in the airline industry last year.

Passengers know where they stand -- whether they have been placed in a separate line, interrogated or searched.

Chakrabarti and Strauss concluded that if a terrorist made six trial flights and got the green light every time, that person could confidently assume that he or she would not be stopped by the system on a real hijack mission.

Schneier suggested an even simpler approach.

"You want a good identity? Steal it," he said. A recent report from the Federal Trade Commission found that 27 million Americans have been victimized by this type of fraud in the last five years.

MIT professor Arnold Barnett, a consultant to the government on aviation safety and security issues, said no computer program is immune to such methods.

"The belief that penetrating people's minds is the key to stopping airline terror could be an illusion that, if taken seriously, might someday be shattered at great cost," he wrote in an upcoming article in the journal Risk Analysis. "In the worst-case scenario, [CAPPS II] could be reminiscent of the Maginot line."

The TSA's Loy said his agency can foil the terrorists' efforts. "We will be counter-gaming the gaming," he said.

One way to do that is to conduct random security checks, which flag passengers regardless of their threat rating.

Random checks were increased after the Sept. 11 attacks, but proved endlessly irritating to the millions of innocent travelers who resent security guards rummaging through their underwear and other personal effects. They have since been "radically" reduced, and would remain at current levels under CAPPS II, Loy said.

CAPPS II would also constantly update its data and adjust its analysis to keep terrorists off balance, Loy said.

But Stanford University computer scientist Jeffrey D. Ullman said that building a prescient computer system capable of seeing through simple human ruses would require an effort comparable to the Manhattan Project during World War II to build the atomic bomb.

Short of that unlikely prospect, the other option is to engulf ever greater amounts of data in hopes of bolstering the computer system.

Privacy Concerns

In its initial plan, the government proposed keeping CAPPS II dossiers of air travelers on file for 50 years, but the idea was dropped after a public outcry.

Privacy advocates still worry that, as with any large database, there is an inevitable tendency to use the information for more and more purposes. Homeland Security chief Tom Ridge, for example, has already approved the use of CAPPS II to identify fugitives wanted for violent crimes.

Even before the deployment of CAPPS II, a major data-security lapse has jolted the traveling public. JetBlue Airways Corp. admitted recently that in a deliberate violation of its own rules, it had secretly delivered detailed passenger data to a military contractor working on a separate airline security project.

Outraged customers have filed suit against the company, and the Homeland Security Department has initiated an investigation.

The TSA acknowledged that some mishaps involving accuracy and disclosure of CAPPS II data are inevitable. The agency will have a passenger advocate and appeals process, but has yet to spell out what rights passengers will have. Congress has asked the General Accounting Office to investigate if CAPPS II can identify suspicious travelers without trampling the rights of innocents; lawmakers are awaiting the GAO's verdict before approving deployment of the system.

"We here at the Department of Homeland Security are also citizens, and we are also very concerned about our rights, about our privacy and about our civil liberties," said Nuala O'Connor Kelly, the department's chief privacy officer.

But privacy advocates say that because CAPPS II information would be classified, travelers would never be certain why they were flagged. It's a Catch-22 that would present enormous challenges for clearing their names -- and an enormous temptation for misuse, said David Sobel, general counsel of the Washington-based Electronic Privacy Information Center.

"People are going to want to know, 'Why am I pulled aside every time I take a flight?' " he said. "The answer is going to be, 'Sorry, we can't tell you.' "

Caption:
GRAPHIC: Computer hunt for terrorists
CREDIT: Los Angeles Times
PHOTO: FREQUENT FLIER: Rep. Peter A. DeFazio (D-Ore.) is a member of the committee overseeing airline security. As an air traveler, he has found that the profiling system can be tricked.
PHOTOGRAPHER: Dennis Drenner For The Times

Record Number: 000063935