THE NEW YORK TIMES

February 26, 2007

Adding to Security but Multiplying the Fears

By ADAM LIPTAK

Foreigners arriving at the American border must present both index fingers for fingerprinting, but that will soon change. The Department of Homeland Security now wants 10 fingers.

The two-print system was largely a biometric backup, an added level of security to supplement and verify a passport or a visa. The 10-print system adds a powerful investigative tool.

“When we have a fingerprint of a terrorist who has left behind a bomb or an I.E.D. in Iraq or has left his fingerprint in a safe house somewhere, we don’t always have the two index fingers,” Paul Rosenzweig, a Department of Homeland Security official, said at a briefing in December. “It could be the pinkie or the thumb. And thus by moving to a 10-print system, we will enhance our ability to use biometrics to enable us to identify threats before they occur in the United States.”

Call it biometric mission creep.

People concerned about privacy and civil liberties say they fear the creation of gigantic biometric databases ripe for data-mining abuse. They note that Mr. Rosenzweig was a supporter of the Total Information Awareness program at the Defense Department, which had planned, as the Pentagon put it, to create “ultralarge all-source information repositories.” The program was shut down in 2003 because it scared people.

The administration’s last-ditch defense of that effort was telling, too. It changed the name to the Terrorism Information Awareness program.

There is a pattern here, said Marc Rotenberg, the executive director of the Electronic Privacy Information Center. “These techniques that are sold to us as necessary to identify terrorists inevitably become systems of mass surveillance directed at the American people,” Mr. Rotenberg said.

In an interview, Robert A. Mocny, the acting director of U.S.-Visit, the unit in the Department of Homeland Security that is in charge of the fingerprint program, said all the right things. “We cannot,” Mr. Mocny said, “have a reaction to 9/11 such that we’re sacrificing privacy and civil liberties on the altar of security.”

But the privacy folks have a point. Once information is captured, it must be tempting to use it. With little discussion, for instance, driver’s license photographs have been dumped into enormous digital databases, ripe for searches with facial recognition technology. Police departments have started to use the databases to find people and identify suspects. That may be a fine idea, but it is one that has been pursued without real debate or disclosure.

Mr. Mocny made a persuasive case that the move to 10 prints enhanced the legitimate goals of identification and investigation.

“We’ve identified 1,800 people who’ve tried to lie their way into the United States, and their fingerprints tripped them up,” he said.

The 10-print program will, he said, make identifications even more reliable. “We’re now at 80 million-plus individuals in the system,” he said. “With that many fingerprints, they start to look alike.” More fingers, he said, means more differentiation.

On the investigative side, more fingerprints give the authorities more opportunities to check them against a watch list of 2.5 million prints that includes, he said, “known and suspected terrorists,” sexual predators and people wanted on criminal and immigration charges.

But there are real questions about the reliability of the technologies employed. Though fingerprint evidence is widely assumed to be close to infallible, recall the $2 million the federal government paid in November in the settlement of a lawsuit filed by Brandon Mayfield.

Mr. Mayfield, a lawyer in Oregon, was arrested in 2004 after the F.B.I. definitively and mistakenly concluded that his fingerprints matched one taken from a plastic bag containing detonator caps found at the scene of the bombings in Madrid that year.

“Fingerprints work fine when you have a bank robbery in Chicago,” said Michael Cherry, vice chairman of the digital technology committee of the National Association of Criminal Defense Lawyers. But matching a partial fingerprint of poor quality and uncertain vintage collected in Afghanistan or Iraq to a database of global scope is a different matter.

The 10-print strategy, Mr. Cherry said, is a “technical nightmare that will produce many Brandon Mayfields.”

At an American Bar Association conference in November, Michael Chertoff, the secretary of Homeland Security, said the 10-print program “creates a powerful deterrent for anybody who has ever spent time sitting in a training camp and training or building a bomb in a safe house or carrying out a terrorist mission on a battlefield.”

Those terrorists, presumably, will be deterred by not wanting to test the nation’s border security. Or the deterrent may be a different one: encouraging a generation of young jihadists to wear gloves.

“Unless you believe there’s a constitutional right or a civil liberties right to have phony documents or to pretend to be someone you’re not, I don’t really see the cost in civil liberties,” Mr. Chertoff told the assembled lawyers.

“By the way,” he added, “we’ll be collecting all of your glasses after dinner.”