

Biometric Passports and Facial Recognition (August 2004)

James A. Lewis

Center for Strategic and International Studies

An announcement by the Department of State that it will move to the use of passports that contain a chip with facial recognition data has prompted a series of complaints from privacy advocates and technologists. The principle concern is that facial recognition systems have a high error rate and that State would be better off if it used fingerprints in the new passports.

The recommendation to rely on fingerprints is, unfortunately, divorced from reality. For many people, being fingerprinted is something reserved for criminals. Most Americans have not been fingerprinted and are unlikely to respond favorably to proposals that they allow the Federal government to fingerprint them. In contrast, people are used to and accept being photographed for passports or drivers licenses. Fingerprinting also faces resistance overseas. European privacy groups have come out against biometric passports that use fingerprinting. The U.S. recently began to fingerprint foreign visitors. The result has been outrage from foreign governments and a fall in tourists coming to the U.S. in part due to the new requirement.

Facial recognition, not fingerprinting, is the preferred multilateral approach. The International Civil Aviation Organization, the international body that sets the rules for commercial air travel, has recommend the use of facial recognition technologies, not fingerprints. Canada will test an 'e-passport' with a chip that contains a digital photograph of the bearer. The European Union will require biometric data on all EU passports, in the form of a digital photograph for use in facial recognition (with the option to add fingerprint data later). The German government is testing iris scans for biometric passports, but many people remain uncomfortable with this technology. As in the U.S., the use of photography for identification purposes now has higher public acceptance than fingerprinting or iris scans.

But what of the error rate for facial recognition, which the experts in the press reports say could be as high as fifty percent. First, the error rate drops when the facial scan is done in a controlled setting, like a passport checkpoint at an airport. Facial scans in the 'wild' (i.e. football stadiums, street) have a high error rate, but a situation where a frontal view is required, lighting is controlled and the subject is not moving, the error rate is much lower. Facial recognition software also continues to improve, and error rates will be lower in 2005 or 2006.

Second, if Customs and Border Protection (CBP), the agency responsible for checking passports, adopts the right procedures, errors in facial recognition need not slow down the lines at immigration. If the facial recognition technology works and recognizes you, you walk through in less time that it now takes. If it fails, you are popped into the line that you go through now. The result is a net savings for how long it takes to process a planeload of people. Even with a fifty percent error rate, which is exaggerated, lines at immigration and the wait could be cut in half.

The issue with biometric passports using facial recognition is not the error rate, but the processes that CBP puts in place to handle errors. If CBP treats everyone whose passport fails facial recognition as a criminal, the new technology will clog airports. If CBP starts by using facial recognition as a supplement to the human screening of passports (an inspector 'eyeballs' your face and the passport picture) it now uses, it will speed entry and increase security.

There are larger privacy issues involved in the collection and use of biometric data by federal agencies, but these apply equally to fingerprints and to facial scans. The most important of these is what the government does with the new digital database it will have on its citizens. As a rule, the less it does the better, and the use of the new digital, biometric data for purposes other than immigration should be avoided. It is not clear, however, that sufficient privacy safeguards have been put in place. The U.S. could defuse some of the concern over biometric passports if it would make clear to the public how biometric passport data will be used and how it will be protected.