International Bulletin of Political Psychology

Volume 12 | Issue 12 Article 1

3-29-2002

Biometrics and the Bottom Line for Aviation Security

Editor

International Bulletin of Political Psychology

Title: Biometrics and the Bottom Line for Aviation Security
Author: Editor
Volume: 12
Issue: 12
Date: 2002-02-20
Keywords: Aviation Security, Biometrics

Abstract. This article attempts to identify the utility of biometric technology for variants of aviation security.

In the aftermath of the September 11, 2001 attacks within the United States (US), some US executive and legislative branch officials, leaders of the aviation industry, and security and intelligence analysts have vociferously pushed biometric technology as a significant part of an upgraded aviation security system. Yet this technology might contribute to aviation security significantly less than its proponents assert.

In the aviation security context, biometric technology usually denotes mechanical, computerized, and electrical devices developed to measure physical characteristics of people. The most common characteristics include structural aspects of the face, fingerprints, and most aspects of the iris. The gross utility of biometric technology is based on assumptions that (1) each person has a unique physical signature concerning the face, fingerprints, or iris; (2) the signature can be detected to some "acceptable" level of accuracy; and (3) detection of the signature has significant security implications.

Unique Physical Signature. It is through inductive reasoning that the assumption of a unique physical signature is commonly made. That is, based on a conclusion stemming from observation that so many individuals have the same property--e.g., a unique physical signature--a generalization is made that all members of a class from which the individual cases were taken have the same property. This is the case even if most members of that class have not been observed to elucidate that property.

"Acceptable" Level of Accuracy. All people may have a unique physical signature, but the resolution of relevant technology is not fine enough to discern the signature. The magnitude of false positive and false negative rates also will be crucial in determining what is acceptable along with political and other public policy constraints.

Significant Security Implication. Even if uniqueness and accuracy are reached at the 100% level, proponents of biometric technology must answer the "so what?" question. It may be easiest to do this by positing how the technology can help with populations of "good guys" and "bad guys."

"Good guys" may include frequent flyers and so-called trusted flyers. The idea is that (1) people who have flown often, often at higher price, and/or without negative consequences for aviation security and/or (2) people who voluntarily submit to extensive background investigations--with said investigations coming back "clean"--are biometrically identified. Their biometric identities are placed in a database and these people are then biometrically scanned and compared with their "stored" biometric identities each time they are set to fly.

The premise is that a match of present scanning and database identities suggests that the individual is not a significant risk to aviation security. However, good people can go bad and may already have been bad at the time of the initial database identification--much as seemingly good people commit espionage,

sabotage, murder, and mayhem. In fact, acts of espionage and the like are more frequent than acts of aviation terrorism and often less catastrophic. All the match seems likely to accomplish is facilitate the post-catastrophe investigation. The same would be the case for biometrics applied to "in-house" airport and airline employees in the context of access to restricted areas.

"Bad guys" are the aviation terrorists and others intent on catastrophic aviation security violation--some of whom may be perceived as "good guys" as described above. The attempt to match database and present scan identities is rendered difficult by shortfalls in human and technical intelligence--and prudent selection of terrorist perpetrators by terrorist entities--wherein many "bad guys" will not have been included in the data base. Here, of course, an attempt at a match is not possible.

On a continuum of aviation security threat, biometrics are likely to be least useful against a sophisticated terrorist entity and most useful against someone with a long public history of violent behavior.

The funding of biometric technological products will be significantly helpful to the economic security of the companies receiving the funding. Given that economic security is one part of national security, this conclusion is not necessarily detrimental to the US. However, as with many aviation security initiatives put in place or likely to be since September 11, 2001, the terrorism-related utility of biometric pales before the three necessities of upgrading intelligence capabilities, strengthening and employing counterterrorist assets, and intensifying antiterrorism initiatives through the psychological lens of all foreign policy tools. (See AcSys Biometrics. http://www.acsysbiometrics.com; Dishman, C. (2001). Terrorism, crime and transformation. Studies in Conflict & Terrorism, 24, 43-58; International Biometric Group. http://www.biometricgroup; Mahmood, C.K. (2001). Terrorism, myth, and the power of ethnographic praxis. Journal of Contemporary Ethnography, 30, 520-545; UnisysBioware. http://www.unisys.com.) (Keywords: Aviation Security, Biometrics.)