

10-24-2003

Biometric, Psychometric, and Sociometric Profiling

IBPP Editor
bloomr@erau.edu

Follow this and additional works at: <https://commons.erau.edu/ibpp>



Part of the [Aviation Safety and Security Commons](#), [Defense and Security Studies Commons](#), [International Relations Commons](#), [Other Political Science Commons](#), [Other Psychology Commons](#), [Peace and Conflict Studies Commons](#), and the [Terrorism Studies Commons](#)

Recommended Citation

Editor, IBPP (2003) "Biometric, Psychometric, and Sociometric Profiling," *International Bulletin of Political Psychology*. Vol. 15 : Iss. 8 , Article 2.

Available at: <https://commons.erau.edu/ibpp/vol15/iss8/2>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in International Bulletin of Political Psychology by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

Title: Biometric, Psychometric, and Sociometric Profiling

Author: Editor

Volume: 15

Issue: 8

Date: 2003-10-24

Keywords: Aviation Security, Biometric, Profiling, Psychometric, Sociometric

Abstract. This article articulates basic Issues in developing security-based profiling technologies.

In public discourse, profiling is often viewed as constituting one of four narratives. On the one hand, it is something that works but whose work should not be allowed. On the other hand, it is something that should be allowed but may not work. There are also adherents of two other narratives: that profiling works and should be allowed to work and that it doesn't work and shouldn't be allowed even if it did. All four of these narratives may ignore important Issues as to the nature, utility, and ethics of profiling. It is to these Issues that we should now turn.

At its most basic, profiling denotes identifying human characteristics that contribute to predicting behavior. With this denotation, one should immediately grasp how common profiling is. In fact, it is a constituent of human psychology or, if you will, of human nature. We profile while awake and in our dreams. We profile as a lead into decisions about whom to trust and of whom to be suspicious, whom to love and whom to hate, whom to respect and of whom to be derisive. We profile voluntarily and involuntarily. Is it not, then, apparent that any question concerning aviation security and profiling should address, not whether or not to use it, but what kind to use?

One typological approach is to assume three classes of profiling—biometric, psychometric, and sociometric—that differ only in what information is applied towards behavioral prediction. (As a caveat, note that profiling can also denote predicting non-behavioral information from other non-behavioral information or even from behavioral information. However, these latter sorts of profiling are deemed less useful in supporting aviation security by most experts credentialed by government, professional organizations; recognized as such by their peers and the general public; and appointed as such by themselves.)

In biometric profiling, the information leading to behavioral prediction comprises human physical characteristics. Common examples of these characteristics employed in aviation security programs include features of the iris, finger pads, structural and kinesic elements of the face, and partially overlapping physiological phenomena that can be detected remotely. Sweating, pulse rate, and respiration are examples of common psychophysiological phenomena.

In psychometric profiling, the information leading to behavioral prediction comprises inferred traits as to human cognition, emotion, motivation, and behavioral tendencies, as well as a plethora of observed traits further describing certain behaviors such as speaking and walking. Common examples of how these characteristics are identified in aviation security programs include interpretations of the results of paper-and-pencil personality inventories and interview data collected from that person being evaluated, as well as from collateral contacts of that individual.

In sociometric profiling, the information leading to behavioral prediction comprises interpersonal, intragroup, intraorganizational, and intracultural aspects of an individual's biological, psychological, and social functioning—e.g., academic and work history, criminal record, degree and type of cooperation

International Bulletin of Political Psychology

and competition with other individuals, participation in informal networks, and ethnic identification. A common example since 9/11 has been association of an individual with others who are deemed at risk for violation security—even as one wonders how these others have been so identified save from direct participation in terrorist organizations or networks that have targeted aviation.

It is at this point that we observe the artificial nature of the tripartite model of biometric, psychometric, and sociometric. Some behaviors, such as sweating or hand clenching could be classified as any of the three. Also, one might have to develop and transit through a host of inferences from biometric to sociometric to psychometric and back again in unique sequences, permutations, and combinations before arriving at a useful, behavioral prediction for aviation security. It is, then, much more important to ensure casting a wide net over all possible human characteristics than to intensively and compulsively relegate such characteristics to one class of information. The tripartite metric model should serve only as a mnemonic and organizational tool and jettisoned for another that is more useful at the discretion of the aviation security professional.

At this point, it is time to consider the legal, moral and ethical arguments for and against using profiling—i.e., should we let it work, assuming it works. Given that all people by virtue of being people engage in profiling one might think the very issue is a moot point—unless one seeks to underline the possibility of eternal damnation for all. However, values as to the rightness and wrongness of personal behavior (morality) and of behavior engaged in while performing a social role as citizen, government representative, or security expert (ethics) might dictate that certain kinds of profiling are acceptable or even highly admired, while other kinds are unacceptable or even detestable. The answer to a question of values is ultimately a political question in secular or sacred society and one that depends on a combination of three main moral and ethical calculations. These calculations are the intrinsic goodness or badness of profiling, the intentions of the profilers, and the consequences of profiling. The author believes that moral and ethical calculations lead to a determination of profiling as good and will, thus, continue with an analysis of profiling strategies.

One profiling strategy is to identify information predictive of behaviors relevant to aviation security based on something one believes merely because one believes it. When push comes to shove, many human beliefs are based on no more than this. Because some such beliefs will be correct if only because it is difficult to be wrong about everything, this strategy has long staying power even if it is short on what many people believe to be appropriate analysis.

Another strategy is to identify information as predictive of behaviors relevant to aviation security based on accepting the assertions of some expert source—without seriously critiquing the assertions and the source. Examples of expert sources include religious, scientific, and policy texts, as well as their authors and those cited by these authors including God and Gods. Hitching one's star to the wagon of an expert source may get one far in the aviation security business, but tragedy may ensue when the attribution of expert is an erroneous one.

Yet another strategy is to identify information as predictive of behaviors relevant to aviation security based on one's reason, rationality, and logic—i.e., one's overt and covert styles of relating and associating discrete and continuous elements of information to arrive at conclusions about the nature of the world, one's place in it, and what the world's nature and one's place in it could and should be (deductive logic). The branch of philosophy called epistemology and the area of psychology called social cognition contain examples of the strengths and weaknesses of this strategy.

A final strategy is to identify information as predictive of behaviors relevant to aviation security based on one's sensory and perceptual observations (empiricism)—whether systematic or unsystematic. As a significant problem with reason, rationality, and logic relates to the vulnerabilities of deductive logic, a significant problem with empiricism is its basis on inductive logic—coming to a general conclusion based on a finite number of specific observations. Because a finite number of specific observations may miss other observations that are exceptions to the generalization, an aviation security program based solely on this may topple like a house of cards—especially against a sophisticated terrorist threat that intentionally looks for such exceptions.

As the tripartite model for classes of information metrics is not a clean conceptualization but masks how the same piece of information can be placed into more than one class and how inferences about such classes can traverse all such classes, so goes the organization of profiling strategies. One can quickly grasp that one can observe and associate observations, rely on expert sources but test them through observations, believe because one believes but subjects these beliefs to reason, and so on.

But even in the face of many different classes of profiling information and profiling strategies and different approaches to describing and analyzing them, aviation security authorities seem to employ only three kinds of profiling systems—again in a context wherein these systems can be mixed as considered appropriate by their developers, employers, and developers. (And these systems characterize the only two purposes that profiling can address. One is whether a person is who that person claims to be. This is most often the basis of employee identification and trusted traveler programs. The other and far more difficult purpose is to gauge the intentions of travelers and employees.)

The first system is based on information about people that can never be or at least not easily be changed. Examples include skin color, actual family background, and original nationality.

The second system is based on past behaviors varying in temporal distance from the time of profiling. Examples include buying a one-way versus a round-trip ticket, attending a meeting of terrorists years before, or living with suspicious characters at some point in time.

The third system is based on observing behaviors initiated with arriving at an airport, checking in, going through security, waiting at the boarding area, and boarding an aircraft that seem to be compatible with specific types of terrorist operations. Examples include body posture concurrent with carrying a weapon, external psychophysiological indicators suggestive of situation-dystonic stress, hand positions unusual for most passengers that may suggest incipient weapons utilization, and spatio-temporal positioning of one's body in an area conducive to injure the most numbers of people.

A significant point of controversy entails how to communicate the accuracy and inaccuracy of various profiling systems. Some system advocates will state that their system is X% accurate. Given that there are two sorts of errors—missing the security threat and falsely identifying one—a single accuracy value is misleading. For example, one can arrive at a 100% accuracy rate of never missing a security threat by identifying all people as a security threat. And one can arrive at a 100% accuracy rate of never falsely identifying a security threat by never identifying anyone as a security threat. In fact, the latter has much to recommend itself, because the great majority of passengers and staff will not pose a security threat.

A last point relates to the perishability of profiling systems. Even if one arrives at a reliable and valid system that has acceptable error rates as defined by what is politically acceptable, these rates are by no

International Bulletin of Political Psychology

means permanent. Sophisticated terrorist threats and mass media representatives can identify the information and interpretive strategies founding a profiling system through reconnaissance, surveillance, and research. And because people change with time and because events help color how they change, information with predictive validity at one point in time may have little or different validity later on and may vary over and over again in degree of validity. The implication is that profiling is a continuous, adaptive enterprise. One learns from success and failures, from better analyses, and most of all from better threat-related intelligence. (See Alison, L., Smith, M. D., Eastman, O., & Rainbow, L. (2003). Toulmin's philosophy of argument and its relevance to offender profiling. *Psychology, Crime & Law*, 9, 173-183; Davis, J.A. (1998). Profiling the Clairemont serial murder case: A collaborative investigative effort. In R.M. Holmes & S.T. Holmes, (Eds.). *Contemporary perspectives on serial murder*. (pp. 149-172). Sage Publications, Inc.; Hart, J. L., Larsen, A. M., Litton, K. S., & Sullivan, L. J. (2003). Racial profiling: At what price? *Journal of Forensic Psychology Practice*, , 79-88; Macias, J. (2002). The tragedy of terrorism: Perspective, reflection, and action in the aftermath. *Anthropology & Education Quarterly*, 33, 280-282.) (Keywords: Aviation Security, Biometric, Profiling, Psychometric, Sociometric.)