HARVARD INTERNATIONAL REVIEW

Behavioral Profiling and the Biometrics of Intent

Nayef Al-Rodhan June 17, 2016 Americas

“Sergeant identifies Baghdaddi city council member with iris scanner” by Michael Q. Retana. CC BY-SA 3.0, accessed via Wikipedia Commons.

Behavioral science acquired a particularly important role in security and defense systems following the 9/11 terrorist attacks in the United States. First and foremost, the attacks were clear evidence of the failure of early detection systems in air transportation. In response, in 2007, the Transportation Security Administration created new positions of “Behavioral Detection Officers” who were tasked to assess passengers waiting in line for security checks according to a set of indicators such as levels of stress.

The SPOT program (Screening Passengers by Observational Techniques), which grew increasingly expensive over the years, received significant criticism and proved to a great extent ineffective. Nevertheless, the use of behavioral sciences has hardly been staved off. In recent years, it has also captured the attention and imagination of defense technologies companies looking to develop new biometric systems to detect early intentions of criminal or terrorist acts.

This technology will remind us once again that scenarios from science fiction can easily become reality. While human emotions, intents and beliefs are obviously invisible mental processes, behavioral biometrics aims to scan our intentions. More specifically, this biometric technology hopes to intercept an individual’s hostile intent before it materializes into an actual hostile act. The rationale for deploying a machine which detects adversarial intent is straightforward: intent normally precedes action, and therefore a timely detection of adversarial intent would lead to the prevention of violent acts. In the United States, the so-called FAST system (the Future Attribute Screening Technology) is being developed to remotely detect vital signs and then look

This technology will remind us once again that scenarios from science fiction can easily become reality

for indices of malintent. Scientists working in the defense sector in Canada and other countries are similarly undertaking concrete steps to attempt to develop the same kind of technology.

The `biometrics of intent` takes biometric identification to new heights. Scanning technologies could go well beyond external physical features, and the companies developing them hope to map emotions and intent of the subjects they analyze.

Yet with this breakthrough come serious questions. Is this technology really feasible, and if so, what are the risks of profiling and thus misreading or over-reading intent? Furthermore, what are the likely ethical, moral and legal implications of possible consequential errors?

A new era of biometrics: from fingerprints to behavioral profiling

The field of biometric technologies was initially developed for security purposes. Biometric-based systems mostly use personal physical characteristics (ranging from fingerprints, faces, voices, iris and retinal images to handwritten signatures) to provide automatic and nearly instantaneous identification. This is done most commonly by converting the biometric into digital form and then comparing it against a computerized database.

> **In Iraq, for example, biometrics was widely used to catch entire groups of bomb-makers, and the US military was careful to store and capture iris and DNA information from the most dangerous individuals.**

A 2001 RAND Report described biometrics as “one of the emerging technologies that will help safeguard the nation.” Over the years, biometrics has become increasingly sophisticated, and has grown to be one of the favorite security technologies of the US federal government in various operational settings. In Iraq, for example, biometrics was widely used to catch entire groups of bomb-makers, and the US military was careful to store and capture iris and DNA information from the most dangerous individuals.

The *biometrics of intent*, however, surpasses the traditional scope and ambition of this technology. It ushers in a new era of biometrics, one where cognitive sciences and neurobehavioral insights will be integrated into the screening processes.

In airports, stadiums and other public areas, the measurement of behavioral signals, such as heart rate, breathing, eye movement, body temperature or fidgeting, are expected to help identify and locate potentially dangerous individuals. Some of the devices or sensors for body signals that have already been developed and tested include thermal imaging to screen temperature changes, eye trackers to follow a person’s gaze and measure pupil dilatation, fidgeting monitors, and devices to track heart and respiratory rates. Results from these screenings would be then considered together, and inform the decision about whether or not to proceed with further checks or questioning.

The underlying hope of the biometrics of intent is to serve as `brain-fingerprinting–checking for behavioral intent. This implies building a behavioral databank and new data-measuring metrics with the help of electroencephalographic (EEG) and functional magnetic resonance imaging (fMRI) responses to stimuli (such as a positive, negative or neutral picture). EEG and fMRI are tools to investigate human brain function. EEG detects electrical activity in the brain using electrodes attached to the scalp, while the fMRI is a functional neuro-imaging procedure that analyzes brain activity in relation to blood flow.

If found to be reliable enough, it is hoped that such technology could help determine whether an anxious-looking person at the airport is just experiencing mundane, everyday stress, or if that person is actually dangerous.

The use of EEG recordings for biometric identification is very recent and brings new features into the identification and authentication processes, making existing systems look rudimentary in comparison. EEG scanning is credited above existing systems because, as its supporters claim, "it is confidential, difficult to mimic and almost impossible to steal." EEG records the voltage fluctuation that results in an ionic current flow between the neurons and, as a result, an EEG-based biometric system would provide "brain signatures." Although testing has been limited, recently collected data showed significant accuracy in detecting some mental tasks (such as relaxation or math calculation) in instances when the subjects were requested to perform these tasks without any obvious and overt movement. Nevertheless, a real-time biometric system which uses EEG signals effectively will require enormous efforts of development and optimization.

Behavioral screening – between prediction, prevention and mishandling

Biometric surveillance in general has been the hotbed of much controversy, and the biometrics of intent undoubtedly takes this debate a step further. For many, such technologies are outright expressions of Orwellian scenarios, and their intrusiveness is frightening in its infringement on privacy and civil liberties. If many previous systems of biometric scanning contained some degree of transparency and were visible to those subjected to scanning, biometrics designed to gauge malicious intent could be embedded in parts of infrastructure or furniture. With these systems, passengers in an airport might step on a "smart carpet" or rest on a "smart seat" full of biometric sensors, all without their knowledge.

For many, such technologies are outright expressions of Orwellian scenarios, and their intrusiveness is frightening in its infringement on privacy and civil liberties.

The promoters of the technology claim that, unlike previous security profiling, behavioral profiling is less discriminatory and less expensive, especially if the technology attains a proven level of minimal error. However, these positives are quickly countered by many caveats and warnings.

Behavior predictability based on algorithms and emotion recognition systems (which read and compare facial expressions, then extract features and their motion information) have been tested for years. Yet, they still display limited accuracy when it comes to actually grasping the full range of human emotions and facial expressions. The biometrics of intent purports to go as far as differentiating between negative and positive states and then beyond, within negative states, claiming the ability to discern the differences between anger, sadness and fear. As powerful as such technology might prove, critics will be comforted to know that such measurements of emotional states remain impossible with the technology currently available.

A few scientific gaps are particularly arresting when assessing the feasibility of this technology. As hinted at above, the scientific study of intention is still not without its controversies. The connections between, on the one hand, beliefs, desires, aspirations or emotions, and on the other hand, intentions, are not fully clear. While there have been great advances in the understanding of the psychophysiology of emotions, these coexist with divergent taxonomies of human emotions, as well as their translation across different cultural contexts. As a result, there are approaches which pigeonhole sets of basic human emotions (happiness, pleasure, etc.)—which are considered to be cross-culturally consistent—as having clear nervous system activity and distinct facial expressions.

Some of the discrepancies in these approaches have found common terrain with EEG and fMRI techniques. These have managed to provide conclusive findings showing that emotional valence is lateralized and that there is an asymmetrical management of emotions. The findings suggest that the right frontal hemisphere is more involved in negative emotions, and the left in positive emotions. The results offered by EEG and fMRI scanning have given unprecedented insights, but the range of correlations and data acquisitions with these technologies still requires more empirical demonstration.

The way forward

The risks due to miscalculations, wrongful accusations or tracking of innocent suspects are immense.

In addition to the technical difficulties of making such machines viable and accurate, there is another risk of their scope becoming indefinite. From airports, they could be deployed more broadly: soon they could be found in all public spaces, from sporting venues to a local grocery store. Under such circumstances, individual privacy and freedom could be severely affected. Critics of the technology in the US have already signalled its violation of the 4th Amendment, which protects people from unreasonable governmental searches and literally mentions “the right of the people to be secure in their persons.”

While a very ambitious innovation, the actual viability of biometrics of intent remains dubious, and security and societal side-effects should be carefully scrutinized.

Nevertheless, the biometrics industry is large and flourishing, in the private sector, academia and governments. Both giant companies (such as those contracted by the FBI), and small start-ups are keen to cash in on government monitoring plans. There is obvious interest in both expanding the reach of biometric identification and in further diversification. While a very ambitious innovation, the actual viability of biometrics of intent remains dubious, and security and societal side-effects should be carefully scrutinized.

Regardless of the technological inaccuracies and potential civil liberty intrusions offered by biometrics of intent, its development has gone on full speed ahead. This is a an example where the marriage of overzealous policy and private sector economics has pushed aside contemporary societal, ethical, legal—or even scientific—norms and values. Moreover, the privacy issues raised by these technologies (and their potential misuse) are reason enough to call for urgent debates in legal and policy-making forums. We must be vigilant and question if every piece of innovation actually works to our general well-being. We must determine where clear red lines need to be drawn before developing technologies that are immensely costly, politically divisive, and morally repugnant to our societies. The technologies associated with behavioral profiling could lead to unprecedented levels of intrusion into individuals' minds. There is, however, little to reassure us that they would effectively prevent real terrorists from carrying out their plans. Oftentimes, the really determined wrongdoer simply learns to cope with technologies meant to deter them. With such technologies fully operational, we have every reason to imagine terrorists and criminals undergoing training to perfect their skills to conceal their intent, improve their temperament or better manage their stress levels.

While any technology that helps humanity become more secure should be welcomed, no technology or policy that endangers civil liberties should be utilized. It is also wise to remember that in our brave new world, sustainable security anywhere depends ultimately on the attainment of dignity for all, at all times and under all circumstances. No amount of surveillance will prevent insecurities if there are persistent injustices and dignity deficits elsewhere.

Nayef Al-Rodhan

Nayef Al-Rodhan is a Neuroscientist, Philosopher and Geostrategist. He is a Honorary Fellow of St Antony`s College, University of Oxford, and Senior Fellow and Director of the Centre for the Geopolitics of Globalization and Transnational Security at the Geneva Centre for Security Policy. Author of Sustainable History and the Dignity of Man. A Philosophy of History and Civilisational Triumph (Berlin: LIT, 2009), http://www.sustainablehistory.com