Audrey Heffron Casserleigh, Jarrett Broder
Emergency Management and Homeland Security Program, College of Social Sciences, Florida State University

Using Psychosocial Attributes in Terrorist Profiling to Identifying Potential Security Threats

The job of identifying people who might be potential security threats is evolving from an attribute based profile to a personality based profile. Previous methods for profiling possible terrorists used a combination of ordinary flat classifiers and relational information gathered from data systems and limited redundant questioning. While these techniques, which include ethnic and racial profiling, religious profiling and travel pattern analysis, have proven good triggers to warrant further investigation, they fail to provide a holistic rendering of possible threats.

This paper examines the integrated use of personality profiling using psychological and behavioral triggers to identify persons of interest. Only recently adopted in the west because of perceived constitutional conflicts, the invasive questioning technique, combined with computerized monitoring of micro-facial and bio indicators is being field tested. The combined psychosocial questioning and bio/facial monitoring protocol is designed to trigger extremist personality typologies and possible narcissistic rage, common attributes in terrorist personality profiles. This paper will seek to evaluate the basis for this profiling technique and any strengths, weaknesses, or opportunities for improvement.

Finding Malintent

Border security for any country, whether in a state of crisis or not, has always been a challenge. In the United States the border security failures that led to the presence of foreign nationals with malintent, defined as the mental state and intention of an individual planning or intending to cause harm to the US or the general public[1], was amplified by internal security failures that allowed hijackers to board a domestic flight. Since the creation of the Transportation Security Administration (TSA) under the Department of Homeland Security over US$ 65.2[2] billion has been spent on a variety of techniques to improve transportation security. In 2011 alone the TSA spent US$ 8.1 billion[3] in an effort to ensure transportation security. Several different approaches and standards have been adopted and the TSA has begun using new tools that may prove effective, but these are fraught with constitutional and civil liberty conflicts.

There has been an evolution in transportation screening, with 9/11 as the punctuated event that clearly marks a shift in intrusiveness. In the years immediately after 9/11, transportations security focused on flat identifiers that could be easily quantified; where had this person traveled before, what was this person's nationality, what was this person's ethnicity, etc. These flat classifiers proved almost pointless when additional events like the Madrid train bombing[4] included Spanish citizens[5], and the London 7/7 attacks were perpetrated by British citizens.[6] In an effort to more accurately predict who might have malintent, TSA has begun to use tools that look at the psychological state of travelers.

The premise that a terrorist is created, and not born, is almost universal and builds on the understanding of the inherent presence of aggression in man that is constrained by social and societal norms. The environmental influences regarding personality and rational decision

---

1 See *Civil Rights/Civil Liberties Impact Assessment of the Future Attribute Screening Technology (FAST) – interactive and Passive Programs by Department of Homeland Security, December 12, 2011.*

2 The figure was compiled from the TSA budgets (enacted, not proposed) for 2002-2012 as they appeared in the Department of Homeland Security's Annual Budget Report. *See http://www.dhs.gov/xabout/budget/dhs-budget.shtm*

3 Department of Homeland Security budget report for FY 2011, page 17.. *See http://www.dhs.gov/xlibrary/assets/budget_bib_fy2011.pdf*

4 The Madrid train bombings were nearly simultaneous, coordinated bombings against the Cercanías (commuter train) system of Madrid, Spain on the morning of 11 March 2004 – three days before Spain's general elections. The explosions killed 191 people and wounded 1,800. The official investigation by the Spanish Judiciary determined the attacks were directed by an al-Qaeda-inspired terrorist cell, although no direct al-Qaeda participation (only "inspiration" has been established.

5 The loose group responsible for the Madrid train event included three Spanish citizens, who were also ironically police informants. Other members included Moroccan, Syrian, and Algerian Muslims.

6 Three of the 7/7 event bombers were of Pakistani descent, but had been born and raised in England. The fourth member (Lindsay) was 19 year old, born in Jamaica but was a naturalized citizen and had been in England since he was five years old.

making of members in terrorist organizations continues to be an evolving area, especially with regard to individual actors' accounts[7].
Conversely the concept of a terrorist personality or profile builds on Freudian psychology which argues that all human behavior, including aggression, is determined by the level of conflict between the desire for self preservation (the life instinct) and the fear of death, which Freud[8] and Lorenz[9] refer to as the sexual/death instinct. Lorenz's work went further describing specifically terrorist extremist behavior as a possible biological drive that was societally programmed into man as part of his need to survive[10].

The inherent relationship the psychological and the political is an easy assumption for the explanation of extremist behavior, and there is a long history of research on the relationship between personality and politics. The interrelationship between the psychology of narcissistic and politically oriented aggression has been superficially raised by other observers, and include a discussion of the "narcissistically inflated self image".[11].

When we look outside of the psychological, and at the political end of the formula, then the profile of a political terrorist becomes more specific. In general a political terrorist is an actor who craves attention, has a strong sense (usually unyielding) of purpose, is captivated by an intense yearning for self-esteem, and is drawn to or supports a dogma or manifesto without question[12]. The presence of a pure ideal, combined with narcissistic rage, is the ultimate formula for profiling an extremist personality with malintent.

Systems of Identification

---

7 For case histories of the environmental factors contributing to the acceptance of violence in terrorist organizations see; *J. Knutson's "Social and Psychodynamic Pressure Toward a Negative Identity: The case of the American Revolutionary Terrorist" in Y. Alexander and J Gleason's, eds., Behavioral and Quantitative Perspectives on Terrorism ; in S. Possony and L. Bouchey's "Ulrike Meinhof and Psychology of Terrorism" chapter in International Terrorsim; in J. Becker's work Hitler's Children: the Story of the Baader-Meinhof Terrorist Gang; and the autobiographical work of M. Baumann, Terror or Love: Bommi Baumann's Own story of His Life as a West German Urban Guerrilla.*

8 See *Freud, Beyond the Pleasure Principle, 1960 and Freud, Civilization and Its Discontents, 1961*

9 See *K. Lorenz On Aggression. New York: Bantam. 1971*

10 ibid

11 See *Lasch The Culture of Narcissiom. New York: W.W. Norton. 1979*. Lasch believed the Underground Weatherman's domestic dissidence was entirely narcissistic. In addition Charles Gagnon and Pierre Vallieres, two once prominent Canadian terrorists, were known to have "a strong element of narcissism". Although assassination is not traditionally considered a form of terrorism, usually because of the missing support group surrounding the action, former Presidents Ronald Regan's unsuccessful assassinator, Hinckley was later diagnosed with "narcissistic personality disorders" *See Cimins, 1982*.. Despite the large body of literature where the relationship between narcissism and aggression is well defined, categorically linking narcissism and political terrorism is not as common.

12 See *Heffron Casserleigh, 2001, Hacker, 1999*

Globally acknowledged as a country with security expertise, Israel was the primary mentor in the revising of TSA's approach to security protocols. Interestingly, Israel's approach to security screening at key ingress and egress points has little to do with technology and is based on interactions between travelers and security professionals[13]. Israel has very few body-imaging scanners, they don't frisk passengers and they are not concerned about the quantity of fluids being carried by passengers. Instead the Israelis employ a cadre of highly trained professional screening officers[14] that watch the behavior of, interact with, and begin detailed conversations[15] with passengers, averaging 57 minutes per passenger in Ben Gurion airport in Tel Aviv. The Israeli philosophy is that it is more effective to detect a would-be terrorists than to try and find their bomb.[16] The Israelis call their approach "behavior pattern analysis" and have a remarkable record of success with no attacks on air-traffic since 1972[17].

When the United States and TSA began creating a behavior analysis program of their own it faced several unique challenges, one of which was the sheer size and volume of people to be screened; Israel estimated it handles 11 million passengers a year at Ben Gurion, while over 736 million traveled through US airports in 2011[18]. With the average cost of security screening already approaching US$ 26 per person [19], employing additional screeners to spend more time with passengers would most likely increase the overall cost of TSA.

---

13 Israeli security protocol also strongly use racial profiling techniques and spend a significantly greater time with Arab passengers than any Jewish travelers. Even Israeli Arabs are more heavily scrutinized and routinely expect up to three hours to pass through the security layers at Ben Gurion. See *Janine Zacharia Washington Post article on "Israeli air security; easy on most, intrusive for a few" published November 27, 2010*.

14 Israeli airport security officers are hand selected from the Israeli military service and go through an intense nine week training, and are trained to discretely monitor passengers. In addition, many of the screeners, sometimes called "selectors" are not armed and are just stationed at various checkpoints around the airport. See *'Are you a Terrorist' , Mail online, D. Rose retrieved 2/8/2012 from http://www.dailymail.co.uk/home/moslive/article-1336571/Terrorism-Can-really-stop-bomber-asking-Are-terrorist.html*

15 One of the first questions asked at the outer check point is, "How are you?". Additional questions reported by travelers include; Why did you come to Israel? How was your trip? Are you Jewish? How often do you go to Temple? Why is your coat/sweater buttoned up? See *Your Rights at Ben-Gurion Airport Searches published by The Alternative Information Center.*

16 ibid

17 The 1972 attack took place in the Ben Gurion arrivals area when three members of the Japanese Red Army armed with grenades and machine guns killed 24 after getting off a flight from Rome. No plane leaving Ben Gurion has ever been hijacked or blown up.

18 586,091,655 domestic, and 149,915,025 international. *See http://www.transtats.bts.gov/Data_Elements.aspx?Data=1 retrieved on 2/2/2012*

19 This value was calculated using total TSA budget over total US population to represent taxpayers. (US Population in July 2011 was 311,591,917 *See quickfacts.census.gov/qfd/states/00000.html*)

In 2003 TSA began implementing an Israeli modeled program called Screening Passengers by Observation Technique [SPOT] at more than a dozen U.S. airports. The Assistant Secretary of TSA, Kip Hawley, said the program was "…developed and implemented to observe normal passenger characteristics and anxieties and identify anomalies to detect individuals who may be a threat to aviation and/or transportation security". [20] SPOT has been characterized mostly as a behavior-pattern recognition system "rooted in the notion that people convey emotions" through subconscious gestures and facial expressions[21] which ultimately could reveal malintent. However SPOT is not a facial recognition system and like the Israeli model is completely based on the subjective reaction of the screener towards a passenger[22]. Unlike the Israeli program, SPOT training for TSA officers lasts only a week, and those selected for SPOT training were already in the routine employ of TSA as security screeners. SPOT trained TSA Behavior Detection Officers [BDOs] are stationed at airport security checkpoints and employ "non-intrusive means of identifying potentially high-risk individuals"' through observation of travelers.[23]

The core theory behind these behavior analysis techniques is the work of Paul Ekman and Wallace Friesen who codified over ten thousand facial muscle combinations into the Facial Action Coding System (FACS). [24] Within those ten thousand facial combinations Ekman and Friesen determined that humans share seven basic emotions; anger, surprise, disgust, fear, sadness, happiness, and contempt. Ekman and Friesen also determined that notwithstanding purposeful or subconscious attempts to conceal, these emotions appear as micro expressions, which last one-twenty-fifth to one-fifth of a second regardless of age, gender, or ethnicity. Given the basic understanding of facial expressions, SPOT educated TSA BDO's are trained to categorize the micro expressions present on passengers faces and translate them to a score. Given a high enough score TSA BDO officers can then justify additional questioning or possible detention of suspect passengers. To date TSA acknowledges that SPOT trained BDO officers, who number over 3,000 in the US, have not identified any suspected terrorists.[25] However, as of 2010, TSA reported 1,800 arrests for kidnapping, drug smuggling, human trafficking, traveling with false documents and other crimes which have been attributed to the SPOT program. [26]

---

20 See *Aviation Security – Reviewing the Recommendations of the 9/11 Commission*, 109th Congress, 3-4 (2006)

21 See *T. Frank, Experts; Suspects body language can blow their cover*. USA Today, Dec 27, 2006 as quoted in *Othello Error* by Lenese Herbert 2007-2008

22 The biggest difference between the Israeli and US models is TSA screeners must avoid racial profiling. Racial profiling would be in conflict with Title VI of the Civil Rights Act which ensures public funds are not spent in a way that encourages, subsidizes, or results in racial, color, or national origin discrimination.

23 Ibid

24 See Paul See Paul Ekman & Wallace Freisen, Unmasking the Face: A guide to recognizing Emotions from Facial Expressions IX-X, 1 (1975)

25 See *TSA SPOT Program still going strong. Published 5/21/2010 at http://blog.tsa.gov/2010/05/tsa-spot-program-still-going-strong.html retrieved on February 29, 2012*.

The TSA SPOT program, with its emphasis on behavioral profiling, has come under criticism from first implementation as a tool that justifies racial profiling, and possible Fourth Amendment[27] violations. Former Assistant United States Attorney Lenese Herbert writes, "SPOT provides the government with unfettered discretion to select and investigate certain individuals. If public sentiment and history are our guides, SPOT is destined to disproportionately target race, ethnicity, and color, not to detect terrorist activity."[28] She further agues, "Specifically, under SPOT, governmental agents in American airports will overreact to travelers' facial expressions by using FACS to inappropriately characterize disagreeable ones as criminally suspicious." [29] Herbert also brings up the background of the TSA officers who train for the SPOT program, indicating that one trainer was, "A former criminal corrections officer who relies upon his experiences with the incarcerated -- populations that disproportionately consist of people of color -- provides instruction to hundreds of SPOT-trained BDOs"[30]

The question of Fourth Amendment rights and security measures have been debated from the beginning of TSA's creation, but Herbert rejects the Supreme Court "search" standard found in *Katz v. United States*[31]. Herbert argues the SPOT programs', "probing visual examination and investigation of travelers' faces and their expressions by governmental officials, even in public locations (including airports, where travelers are wrongly said to have waived or assumed the risk of losing their Fourth Amendment protections), constitutes a violation of the Fourth Amendment right to be let alone and its prohibition against unreasonable searches and seizures."[32]

---

26 One of the more notable cases was when BDO officers performed additional screening of a nineteen year old Indian woman, this allowed the woman the opportunity to inform an agent of physical abuse at the hands of her father, who was also traveling with her and attempting to take her to India against her will. See *Newark TSOs Help Thwart Kidnapping, Screening Passengers By Observation Techniques, Additional SPOT News & Information,* May 2007, http://www.tsa.gov/press/happenings/newark kidnapping.shtm

27 The Fourth Amendment (Amendment IV) to the United States Constitution is the part of the Bill of Rights which guards against unreasonable searches and seizures, along with requiring any warrant to be judicially sanctioned and supported by probable cause.

28 See *Othello Error: Facial Profiling, Privacy, and the Suppression of Dissent. 5 Ohio St. J. Crim. L. 79 (2007).* Herbert uses the term "Othello Error" to describe when a suspicious observer discounts cues of truthfulness, given the observer's need to conform her observations to her suspicions, which are usually of deception.

29 ibid

30 Ibid . Herbert cites U.S. Department of Justice Bureau of Prisons Statistics, "Inmate Breakdown," http://www.bop.gov/news/quick.jsp#2 (last visited June 22, 2007) to support her claim.

31 389 U.S. 347 (1967). The Court ruled that Katz was entitled to Fourth Amendment protection and that a physical intrusion into the area he occupied was unnecessary to bring the Amendment into play. "The Fourth Amendment protects people, not places," wrote Justice Potter Stewart for the Court. The Court set the standard for searches ruling that a search occurs when 1) a person expects privacy in the thing searched and 2) society believes that expectation is reasonable.

32 ibid

The core of the racial profiling litigation being filed under Title VI of The Civil Rights Act, is the subjective nature of TSA SPOT trained BDO officers. Reading and attempting to quantify micro expressions that occur in less than a second can be difficult to defend. In an effort to reduce subjectivity in screening, TSA has begun field research on a program that uses computers to analyze facial expressions. If the same facial theories that Ekman and Freisen posited for the SPOT program were gathered instead via surveillance equipment, then evaluated and quantified by a computer, the subjectivity of a TSA BDO officer is eliminated. Surveillance cameras and equipment could also allow for expanded screening in crowded areas, and where there may be long lines. Not only could such surveillance systems monitor individuals, it could also detect crowd anomalies and detect individuals, "whose facial expressions are different from the previous two dozen people in line". [33] This expansion of the SPOT concept of passenger profiling, "…would be consistent with emerging trends in security and law enforcement monitoring; the Department of Homeland Security ("DHS") has been channeling millions of dollars to local governments around the country to create hi-tech camera networks that can be linked with private surveillance systems."[34]

Profiling of passenger with malintent who plan or intend to cause harm has become such a complicated undertaking to conduct, quantify, and defend it is understandable TSA would be looking towards computer based solutions. The observations of a SPOT trained BDO officer is only the tip of the ice-berg in information gathering. SPOT trained BDO officers are evaluating the responses and interaction as they engage or observed passengers. While observation may trigger a need for questioning, without interaction there is little data to evaluate. If however, every passenger were to be biometrically screened, the interaction and evaluation time between passengers and TSA BDO officers could be dramatically reduced. TSA has high hopes for these systems and began testing biometric-based security screening techniques as early as 2006. Passengers were evaluated using complex algorithms, artificial-intelligence software, and polygraph principles to ferret out individuals who exhibit certain suspicious physiological responses to automated questioning.[35] In a pilot project in Tennessee, passengers answered questions about their travel plans as they placed their hands on sensory monitors that measured blood pressure, pulse, and sweat levels. [36]

Programs Currently in Testing Phase

---

33 *See* Paul Ekman, *How to Spot a Terrorist on the Fly, Washington Post, 10/29/2006, B03*. "Meanwhile, short-term research on several questions—whether SPOT misses people whose behaviors are on its checklist; whether other behaviors should be included on the list; and whether additional training would increase observers' accuracy—could help improve the program.").

34 See Justin Florence and Robert Friedman, Profiles in Terror: A Legal Framework for the Behavioral Profiling Program. 17 Geo. Mason L. Rev. 423 (2010).

35 See *Transportation Security Administration., Biometrics, http://www.tsa.gov/approach/tech/biometrics.shtm* Retrieved on 2/29/2012.

36 ibid

Biometric identification, which includes retinal scans and fingerprint matching, has expanded, and TSA is currently working with DHS on a new program called FAST – Future Attribute Screening Technology. FAST would analyze additional factors including pheromones, breathing, eye movement, body temperature, and fidget rates. The Department of Homeland Security says the FAST program could determine, "whether you have hidden explosives or whether you're carrying a weapon" by using "sensors and cameras located at security checkpoints" that "measure the natural signals coming from your body—your heart rate, breathing, eye movement, body temperature and fidgeting". [37]

One of the companies pioneering the kinds of technology that can be used as part of the FAST program is WeCU Technologies based out of Northern Israel. WeCU (pronounced as We see you) is an Israeli startup founded in 2003 by a group of academics and professionals specializing in human psychology, stress behavior, advanced technology and terrorism. [38] The system they developed melds traditional behavioral science with advanced biometric sensors to detect human characteristics indicative of a person who "intends to carry out a particular activity or has a significant acquaintance or involvement with a specific threat."[39] During a 2-3 minute screening procedure, the WeCU system initially takes a baseline reading of heart rate, body temperature and breathing rate. The system then exposes a subject to a series of visual triggers in a non-obtrusive manner designed to stimulate the brain in a particular way as to elicit involuntary physiological responses that can be detected by biometric sensors, primarily a thermal camera. If the visuals shown are relevant to the activities the individual being screened is associated with, the body will react with slight increases in temperature, eye movement and micro facial expressions the subject cannot control.[40]

The WeCU system is designed to identify malicious intent and alert screeners that a particular subject might require additional screening or investigation. To ensure accuracy and to prevent potential threats from learning the visual cues displayed by the system, the manner in which visual stimuli are presented to the subject are varied and often incorporated into existing airport processes. For instance, at a security checkpoint kiosk screen, the traveler might be asked, "enter name," but briefly flashes, "enter real name." [41] WeCU CEO Ehud Givon says, "most travelers wouldn't respond to the different prompts, but someone who is hiding a true

---

37 . *See* Pam Benson, *Will Airports Screen for Body Signals? Researchers Hope So, CNN, Oct. 6, 2009, available at http://www.cnn.com/2009/TECH/10/06/security.screening/index.html.* Retrieved 2/29/2012

38 *See About WeCU Technologies*, *available at http://www.wecu-technologies.com/206863/About-us*. Retrieved 3/13/2012

39 ibid

40 ibid

41 ibid

identity would."[42] The tests are designed to elicit a response from subjects with knowledge of an act of terrorism or malintent in regards to their travel as opposed to travelers nervous about flying or some other personal matter. Givon also says, "the more you try to train yourself not to react to the stimulus, the more clearly you will stand out."[43]

The WeCU system has undergone several years of field testing at airports and security check points in Israel with very low false positive rates and a 95% success rate for identifying individuals with knowledge of or with intent to do harm.[44] During its eight year research and development period, WeCU technologies received two research grants from US DHS and three grants from the Israeli Chief Scientist.[45] It currently has a Memorandum of Understanding (MOU) with Penn State University's International Center for the Study of Terrorism for active research cooperation.[46] Rafi Sela, a top security consultant and former chief security officer at the Israel Airport Authority says, "This company has an algorithm that in some countries would be viewed as an invasion of privacy - Canada will never install it. I've told Canada that you can't do security with political correctness. As long as you are doing it without a real plan, it will never work."[47]

Future; Active vs Passive Screening

The Israelis have said if a terrorist makes it to the airport then your government's security apparatus has already failed[48]. This has proven true in most countries where terrorist plots are foiled primarily through early intelligence sharing and traditional community based policing. These active methods have uncovered numerous plots in the US[49] and the next wave of security technology is clearly aimed at active information gathering. The passive method of screening

42 *See* Irin Carmon, *WeCU Technologies Advances Airport Security, FastCompany, 7/21/2010, http://www.fastcompany.com/magazine/147/next-tech-checkmate.html*. Retrieved 3/13/2012

43 *See* David Rose, *'Are you a terrorist?' The simple question being asked at an airport which could rumble a suicide bomber, Mail Online, 12/15/2010,* http://www.dailymail.co.uk/home/moslive/article-1336571/Terrorism-Can-really-stop-bomber-asking-Are-terrorist.html#ixzz1p0pM37LA. Retrieved 3/13/2012.

44 *See* David Shmah, *Sorting the Bad Guys from the Good, Israel 21c, 2/2/2010, http http://www.israel21c.org/technology/sorting-the-bad-guys-from-the-good.* Retrieved 3/13/2012

45 *See About WeCU Technologies*, *available at http://www.wecu-technologies.com/206863/About-us*. Retrieved 3/13/2012

46 *See The Opportunity - Wanted: Intent Detection Systems, WeCU Technologies Ltd., http://www.epicos.com/epicos/extended/israel/wecu/wecu_home.html.* Retrieved 3/13/2012

47 *See* Kloopsterman, *Israel's Top 10 Airport Security Technologies, Israel 21c, 3/15/2010, http://www.israel21c.org/technology/sraels-top-10-airport-security-technologies*. Retrieved 3/13/2012.

48 See *Janine Zacharia Washington Post article on "Israeli air security; easy on most, intrusive for a few" published November 27, 2010*.

passengers immediately before they travel in an effort to find a terrorist means an entire network of events, actions, and possibly even propaganda to support that terrorist were undetected.

With this in mind, the focus of research on terrorism and security threats has sought to actively profile individuals in a given society and monitor them to find potential anomalies. The US government is currently funding research to help identify disgruntled or radicalized individuals residing within the country. One such program in development is the Anomaly Detection at Multiple Scales (ADAMS) [50]project currently being funded by the Defense Advanced Research Projects Agency (DARPA). The premise of ADAMS is to mine enormous datasets in an attempt to proactively identify the warning signs of homicide, suicide or other malevolent behavior. [51] While the technology developed as part of the ADAMS program will have applicability in multiple domains, it will primarily be used to identify insider threats who are currently trusted individuals in a secure environment with access to sensitive information and information systems.[52]

However, funding from DARPA does not stop at keeping track of internal trusted individuals. As early as January of 2002, DARPA established the Information Awareness Office (IAO)[53] as part of a project to bring together several different DARPA funded research efforts focused on applying surveillance and information technology gathering systems to achieve what they called Total Information Awareness (TIA).[54] The idea behind the TIA program was to establish massive databases that would collect information from emails, online purchases, bank transactions, social network interactions, phone calls, medical records and a wealth of other digital and internet accessible sources on everyone in the US without any requirement of a search warrant.[55] IAO research was conducted along five major investigative paths: secure collaboration problem solving; structured discovery; link and group understanding; context aware visualization; and decision making with corporate memory.

---

50 *See DARPA-SN-11-02: Anomaly Detection at Multiple Scales (ADAMS) Industry Day, viewed at https://www.fbo.gov/index?s=opportunity&mode=form&id=be2bd30988083bd622c2e0af807caacc&tab=core&_cview=0*. Retrieved 3/13/2012

51 ibid

52 ibid

53 See *Statement by Dr. Tony Tether, Director Defense Advanced Research Projects Agency, testimony before the Subcommittee on Terrorism, Unconventional Threats and Capabilities, House Armed Services Committee, United States House of Representatives, March 19, 2003.*

54 Later changed to Terrorism Information Awareness Program according to a TIA Executive Summary, *http://www.information-retrieval.info/docs/tia-exec-summ_20may2003.pdf*. Retrieved 3/13/2012.

55 See John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans, The New York Times, 11/9/2002, http://www.nytimes.com/2002/11/09/politics/09COMP.html?pagewanted=all*. Retrieved 9/13/2012.

Although funding for TIA was pulled and the IAO was closed in 2004 amid allegations that it violated the privacy of individuals, the two core programs of the project were moved out of DARPA and into Advanced Research and Development Activity (ARDA), housed at NSA headquarters in Fort Meade, Md.[56] One of the systems, code named *Basketball*[57], is the Information Awareness Prototype System, the core architecture that tied together numerous information extraction, analysis, and dissemination tools developed under TIA. The other program is code named *Topsail*[58], formerly Genoa II under DARPA. Topsail's primary function focuses on providing information technologies to help analysts and policy makers anticipate and preempt terrorist attacks.

After *Basketball* and *Topsail* were transferred to the research wing of the NSA, little is known about the progress of these projects, but DARPA is still funding research into technologies for gathering, storing and analyzing information gleaned from online sources. One such project is the Social Media in Strategic Communication (SMISC)[59] project, which according to public solicitation notice released July of 2011, states the SMISC will accomplish four major goals:

1. Detect, classify, measure and track the (a) formation, development and spread of ideas and concepts (memes), and (b) purposeful or deceptive messaging and misinformation.
2. Recognize persuasion campaign structures and influence operations across social media sites and communities.
3. Identify participants and intent, and measure effects of persuasion campaigns.
4. Counter messaging of detected adversary influence operations.[60]

The placement of research projects, contributing to the TIA concept, under the NSA means any progress, protocols, and results are completely "black boxed"[61] - unavailable to the public. It is clear this research could be beneficial, and variations of the TIA and ADAMS program are being tested in US occupied countries like Afghanistan and Iraq. However, use on domestic soil begs the question if the government is collecting a baseline of these attributes for individuals to create a national database that can be used for suspect questioning outside of transportation and border security.

---

56 See Mark Williams, *The Total Information Awareness Project Lives On, Technology Review, 4/26/2006, http://www.technologyreview.com/energy/16741/?p1=A2.* Retrieved 3/13/2012.

57 See Shane Harris, *TIA Lives On, National Journal, 2/23/2006, http://shaneharris.com/magazinestories/tia-lives-on/*. Retrieved 3/13/2012.

58 ibid

59 See Solicitation Number: DARPA-BAA-11-64, *https://www.fbo.gov/utils/view?id=260a47e592fc4e0bb25207af167c13f3, 7/14/2011*. Retrieved 3/13/2012.

60 ibid

61 An old NSA term reflective of

Conclusion

As technology has progressed to a point where the government is able to easily intrude into our personal lives, the law has sought to maintain an acceptable balance between the needs of law enforcement and constitutional rights.[62] A joint report from the National Research Council states, "one finds that since 9/11, public opinion surveys reflect a diminishing acceptance of government surveillance measures, with people less willing to cede privacy and other civil liberties in the course of increased terrorism investigation and personally less willing to give up their freedoms and more pessimistic about protection of the right to privacy."[63] Public opinion polls indicate that Americans have a tendency to defend civil liberties in the abstract sense than as it pertains to a particular situation. They are also less concerned about privacy in general unless it pertains to their own privacy and are not concerned with monitoring and surveillance equipment used, so long as it is not used in activities they are involved with.[64] This dichotomy of opinions presents a tremendous hurdle for law enforcement and litigators to overcome.

While the systems profiled here point to a government able to actively identify threats, and possibly prevent terrorist events, the collection of data on citizens at this level brings to mind an Orwellian[65] state where people could be detained for their thoughts. The FAST program is already facing challenges under the Fourth Amendment and the Civil Rights Act, and it is clearly understandable the civil liberties uproar the TIA program created.

While the practice of using psychosocial attributes for helping to identify persons with malintent is a proven method for reliably selecting subjects at security checkpoints, the TSA's use of it through the SPOT program may not have been the best implementation of behavioral threat detection.[66] The use of technology to augment this process shows great potential for more accuracy, less false positives and less inconvenience for those being screened. Coupled with lower costs for operation, decreased wait times for travelers and less training on the part of security personnel for identifying psychosocial attributes, many of these technologies may ironically make the civil rights concerns moot.

---

62 *See Protecting Individual Privacy in the Struggle Against Terrorists:A Framework for Program Assessment, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council. Page 10. 2008*

63 ibid

64 ibid

65 "Orwellian" describes the situation, idea, or societal condition that George Orwell identified as being destructive to the welfare of a free society. It connotes an attitude and a policy of control by propaganda, surveillance, misinformation, denial of truth, and manipulation of the past.

66 *See* Matthew Harwood, *$385 Million TSA Program Fails to Detect Terrorists: Behavioral Profiling Project is Pseudoscience, truthout, http://archive.truthout.org/385-million-tsa-program-fails-detect-terrorists66213*. Retrieved 3/13/2012.

It has long been recognized that innovation moves faster, and often pushes the boundaries of, legislation and law. As governments continue to push the limits of technology in an attempt to keep us safe, it is only through an understanding of these technologies that we can preserve the balance of rights and safety.