Article

Recognizing Friend and Foe: Biometrics, Veridiction, and the Iraq War

Stefka Hristova

Michigan Technological University, US.
shristov@mtu.edu

Abstract

In analyzing the deployment of biometrics in Iraq, argue that whereas the body was seen as a site of verification in 20th century surveillance and identification practices, in the ongoing War on Terror, and the Iraq War more specifically, it became a site of veridiction—a site in which the truth about the security of the state can be analyzed (Foucault 2008: 32). The body thus became the basis for determining not so much one's unique identity but one's friendliness to the normative state order. Enemies could thus be identified and confined as a group, and in this process the state could be secured. In the ongoing of the War on Terror, the visual regime of veridiction has been further articulated to the logic of digital technologies in order to categorize an unfamiliar diverse population into a binary simplistic schema consistent of true and false, therefore friend or foe, and thus “go”—allowed to move through the country—or “no go”—destined to be detained. In other words, the digitization of veridiction as the primary goal of biometrics is evident in the automation of the recognition method, the conversion of the archive into database, the transition away from the anthropological station onto mobile dispersed data-gathering enterprise, and replacement of scientific expertise with easy-to-use automated intelligence.

Like technology from the latest spy movie, a system using finger prints and retina scans helps soldiers tell the difference between the good guys and the bad guys in Iraq.

Chad Cooper, *The United States Army* (January 7, 2010)

Introduction

In 2007, American soldiers in Iraq complained that both Iraqi allies and al-Qa'ida members “looked identical, wore similar sweat suits and carried the same kind of guns” (Cordesman and Davies 2008). In order to distinguish friend from foe, they required their supporters to wear white headbands and ride in Strykers. The white headband was adopted by the enemy and a new mode of identification was issued for the Iraqi forces: reflective armbands. The armbands however proved insufficient means of identification and Iraqi fighters were asked to provide to the Americans their fingerprints, addresses, and retina scans so that the U.S. military “could track down anyone who betrayed [it]” (Partlow 2007). The biometrically obtained fingerprints were compared against Saddam Hussein's old criminal database—foes of the state during Saddam's regime were looked at with suspicion by the American administration (Shachtman 2007). In the face of extreme difficulty in distinguishing friend from foe and the pressing need to establish Iraqi allies, the American militarized state-building enterprise turned to the science of precise body measurement. Today, the United States owns a biometric database featuring the “names, facial scans, and often other details [...], such as whether they were considered a friend or foe” of 3 million Iraqis (Stockman 2010). Even though the Iraq War is over, this database will remain in indefinite possession of the US Central Command (Acherman 2011).

The 2003-2010 American administrations of Iraq attempted to achieve easy and yet reliable recognition of Iraqi subjects in order to quickly and efficiently distinguish Arab allies and enemies. The US mission in Iraq deployed simplistic binary dichotomy juxtaposing friend to foe, true to false, and “go” to “no go” labeling. This schema was meant to determine one’s status in relation to the security apparatus of the state and further curtail the movement of those deemed to pose danger to the state. From the beginning of the Iraq War on March 19, 2003, the US military engaged in massive capture and detention operations. By April 2003, US military personnel were sorting thousands of captives into categories (civilians, security detainees, and unlawful combatants) in order to forward them to the appropriate detention facilities (Locy 2003). As interrogation and torture were rendered standard, yet not very effective, information-extracting practices, the process of recognition required the development and elaboration of surveillance systems that could both capture and analyze the body—a masculine body that is taken as a universal body—and its visual indexes. I argue that whereas the body was seen as a site of verification in 20th century surveillance and identification practices, in the ongoing War on Terror, and the Iraq War more specifically, it became a site of veridiction—a site in which the truth about the security of the state can be analyzed (Foucault 2008: 32). The body thus became the basis for determining not so much one’s unique identity but one’s friendliness to the normative state order. Enemies could thus be identified and confined as a group, and in this process the state could be secured. In the ongoing of the War on Terror, the visual regime of veridiction has been further articulated to the logic of digital technologies in order to categorize an unfamiliar diverse population into a binary simplistic schema consistent of true and false, therefore friend or foe, and thus “go”—allowed to move through the country—or “no go”—destined to be detained. In other words, the digitization of veridiction as the primary goal of biometrics is evident in the automation of the recognition method, the conversion of the archive into database, the transition away from the anthropological station onto mobile dispersed data-gathering enterprise, and replacement of scientific expertise with easy-to-use automated intelligence.

The Body as Site of Veridiction

The “unidentifiable” enemy is a construct that gained prominence in the US discourse in the aftermath of the end of the Cold War. It has become the predominant paradigm in speaking about the threat to the state in the aftermath of 9/11 (Gates 2011). This construction of the enemy as both unknown and highly mobile is intimately connected with the post-Cold War shift from war between two main “blocks”—East and West—to an asymmetric war in which states are threatened by non-state actors. More specifically, the “unidentifiable” mobile enemy is connected with the articulation of “failed states”—countries “without leadership, without order, without governance itself” (Altwood 1994). In other words, “failed states,” by virtue of the lack of strong government, are seen as empowering a new kind of enemy that is both “unidentifiable” and highly mobile and therefore are propagating asymmetrical warfare. Strong governments hold their populations in check by restricting mobility out of the state through severe emigration measures, whereas weak or failed governments are seen to pose danger to the global world order precisely because they have fluid borders. The perceived lack of legitimate sovereignty in “failed states” raises the question of the institution of surveillance as a form of imposed sovereignty that would guard against the undesired movement and actions of the foe. Militarized state-building thus takes on the task of managing “failed states” through surveillance and immobilization in order to secure not necessarily the state itself, but rather a Western *nomos* and the Western civilized state more specifically. Enemies of the state, hence to the global world order, are to be first identified, and second contained.

Militarized state-building past and present relies on the visualization and the subsequent classification of large population groups. It requires each member of the newly established state to truthfully answer the question: “Who are you?” The gathered responses are meant to distinguish between the simplistic binary dichotomy of friends and the foes of the state. Because of the suspicion that one might not always answer the question “Who are you?” truthfully, more objective means of judgment have historically been perused. In other words, verbal and written self-disclosures have been seen as the most malleable and thus

unreliable method of identification. Objective truth was to be found in the body and the indexical properties of the body. More specifically, truth lies in the body's universal, unique, permanent, and collective traits.

In the context of Iraq, although the body's features remained the primary site of identification during the Iraq War, the nature of the information gathered through this identification has shifted radically from the dominant paradigm of the early 20th century which evoked processes of verification. The body, via an analysis of face through precise facial measurements, facial recognition, and iris scans on one hand and of the visual indexes casted by the body—namely fingerprinting—and photography on the other, has been transformed not only into a site of verification, but more profoundly, into what Foucault terms “a site of veridiction” (Foucault 2008: 32).

Foucault uses the term veridiction to uncover the emergence of governmentality—“a new art of government [in which] the organization of numerous and complex internal mechanisms whose functions [...] is not so much to ensure the growth of the state's forces, wealth, and strength, to ensure its unlimited growth, as to limit the exercise of government power internally” (Foucault 2008: 27). He argues that during the 18th century it was the market that became the locus of this new truth regime as it was through an assessment of the market as good and bad that the efficacy of the government can be measured: “[t]he market must tell the truth (*dire le vrai*); it must tell the truth in relation to government practice” (Foucault 2008: 32). In other words, the market, as a site of veridiction, became “a site of verification-falsification for governmental practice,” of determining “correct” and “erroneous” government practices based on a standard of truth rooted in the prices in a market. The natural mechanisms of the market thus constructed a “regime of truth” that could “falsify and verify” government practice.” (Foucault 2008: 32). I extend Foucault's notion of veridiction in relation to governmentality to the context of the 2003-2010 Iraq War in order to illuminate the ways in which militarized state-building in Iraq sought a regime of truth grounded in the individual body. The verification and falsification of government practice was to be based on the identification of Arab friends and foes. Whereas verification in relation to the body has historically been connected to unique identification and complex classification, in the context of veridiction, verification is always and already coupled with its opposite—hence falsification. The militarized governmental practices in 2003-2010 Iraq were to be measured as correct or erroneous based on the ability to endow each foe of the state based on a binary simplistic “enemy/friend” labeling system, rather than based on the ability to endow each foe with a unique identity. In other words, the efficacy of US-led governmentality in Iraq, which attempted to establish a secure country both through the growth of the disciplinary state forces as well as through the curtailment of US influence under the banner of the forthcoming free Iraqi state, was to be measured based on the occurrence and positioning of naturally existing foes of the state.

Foucault further argues that veridictional questions were installed in the heart of the modern penal system through the replacement of the question “What have you done?” with the question “Who are you?” (Foucault 2008: 34). The question “Who are you?” was to provide a regime of truth for the penal system, rather than directly for governmental practice. As Joseph Pugliese has eloquently argued, the question “Who are you?” becomes the “foundational question of biometric technologies” and “is repeatedly made coextensive ... with the question *what are you?*” (2010: 1). Building upon the work of Foucault and Pugliese, I position biometrics as a technology not only of verification, but also of veridiction.

I argue that in the 19th and early 20th centuries “Who are you?” functioned as a site of veridiction as to one's criminal status in the context of the penal system and as a site of verification of one's unique identity and complex cultural categorization within the larger state apparatus. Whereas in the late 19th century identification was equated with verification as exemplified in Craig Richardson's study of the US Passport, I argue that in the late 20th century verification was further reduced to a regime of truthfulness *in and of itself* (Robertson 2004: 454; Robertson 2009: 331). Whereas in regimes of verification the question “Who are you?” was meant to reveal one's unique identity and cultural belonging, in the current

veridiction-driven military state-building processes, such as the Iraq War, it imposes a binary response: an Arab ally, or an Arab enemy. Regimes of truth grounded in the public and individual body previously directed to the penal system are now directly connected to a militarized governmental practice, de facto extending the penal logic as state logic.

The transposition of the logic of veridiction that was once limited to the penal system and the market to governance in the context of occupation more broadly reflects a shift away from “*societies of sovereignty*” to “*societies of control*” (Deleuze 1992: 3, 4) and speaks to the neoliberal nature of militarized state-building. In this new social order, according to Deleuze, “[I]ndividuals have become ‘*dividuals*,’ and masses, samples, data, markets, or ‘*banks*’” (1992: 5).

In the context of the Iraq War, the Iraqi population was reduced by biopolitical biometric technologies to binary data, indicating friend or “go” and foe or “no go” status, to be housed in a US-managed 3 million entries database. The dyadic format of the outcome of the biometric scan based on the collected data speaks to the veridiction role of biometrics in Iraq. Pugliese writes that,

[A]s a biopolitical technology, iris scan effectively disciplines the body of the such subjugated Iraqi civilian though the enforced prising open of her or his eyelid; simultaneously, the scanned template is inserted within the networked grid of biopolitical intelligibility which claims to identify ‘friend from foe’ and thereby sort population groups according to an imperially imposed series of categories and classifications.
(2010: 92)

The series of categories in Iraq were reduced to a regime of truth that ultimately seeks to distinguish friend from foe. In reducing the individual to dichotomous binary digital data, biometrics in this case ultimately has helped to secure a neoliberal *society of control*.

The Body, The Archive, and the Database

Militarized state-building relies on the systematic classification of populations. This classification has historically been linked to a mode of surveillance visualization that is predicated upon the cellular spatial distribution of individuals. In other words, as Foucault as argued, “*tableaux vivants*” or living tables/living grids of specification lie at the heart of the disciplinary project (Foucault 1995: 148). Grids, and tables by extension, are “systems according to which the different kinds of [objects] are divided, contrasted, related, regrouped, classified... as objects of ... discourse” (Foucault 1969: 42). Historically, both anthropometry and biometrics rely on the cellular organization both of individuals and of the gathered data about them. The two identification systems utilize cellular technologies of data-gathering and data-organization: namely disciplinary institutions such as the hospital, the camp, and the prison and the technology of the database. With the emergence of the digital database however, the process of data-organization becomes structured by an invisible grid—the “*tableaux vivant*” and its sorting mechanisms have been obscured.

Historically, the individual human body, as a site of verification and veridiction, has been identified and classified in relation to the “truth-apparatus” (Sekula 1986:16) constituted by the archive as theorized by Michel Foucault (Foucault 1995) and the database as conceptualized by Mark Poster (Poster 1990). In the 19th century, photographic portraiture came to “establish and delimit the terrain of the *other*, to define both the *generalized look*—the typology—and the *contingent instance* of deviance and social pathology” (Sekula 1986: 7). These processes were made possible by the linkage of photography to a “truth-apparatus” as the “camera is integrated into a larger ensemble: a bureaucratic clerical-statistic form of ‘intelligence.’ This system can be described as a sophisticated form of the archive” (Sekula 1986: 16). As Foucault has argued, a disciplinary society is built upon the knowledge obtained through observation and

examination and stored into a retrievable archive (Foucault 1995: 189). In other words, both verification and veridiction knowledges are produced as they are being collected (Robertson 2004: 454). However, in the digital age, the archive has been transformed into an automated retrievable duplicable database (Poster 1990: 94). Thus the processes of observation and examination today are intimately connected with the authentication of this information against a reliable database. In the case of the use of biometrics during the Iraq War in Iraq, it is the construction of the database in the process of data-collection, not the observer's subsequent recordings that determine one's status as friend or foe.

The biometric research conducted by the US Administration of Iraq was stored in a digital database, isolated from cultural analysis of the findings. Whereas the archive, driven by the filing cabinet and the digital file folder, provided means of organization, the database with its "pure grid" structure provided means for automated computerized comparison (Poster 1996: 185). The two technologies together constituted a disciplinary framework that integrated photographs, fingerprints, and physical and behavioral data.¹ The digital database renders the digitized body into an invisible computer, rather than visible scientific, algorithm. A database "arranges information into rigidly defined categories or fields" where the fields or categories are arranged into vertical columns while information is represented in horizontal rows (Poster 1990: 96). In the digital context, the arrangement of the database into rows and columns, as well as the "relationships among pieces of information that do not exist outside of the database" remain invisible to the common user (Poster 1990: 96). Whereas the analog database functions as a visible living table, the digital database renders it invisible to the human eye and visible only to the logic of the computer.

The database provides an organizational structure in which each individual uniform record could be easily retrieved. Its size is representative of the archive of gathered data. An analog archive visualizes the volume of records, without exposing the contents of each entity. Similarly, the digital archive can provide listings of its content without the display of the content of each entity. Its scope and size however are dematerialized and expressed in abstract digital storage measurement units. The digital archive, however, can be hidden from view with much greater ease.

The comparative structure of the database expands beyond its own limits. Through their relational structure (the existence of standard fields across multiple databases), databases can be combined with other databases, "forming vast stores of information that constitute as an object virtually every individual in society" (Poster 1996: 186). In the context of the Iraq War, the database gathered by the US military was relationally linked to the criminal database maintained by Saddam Hussein in order to determine one's true standing as a friend or foe of the state.

The digital database impacts not only the logic of comparison, hence identification, verification, and veridiction, but also the results that this logic produces. The binary code of the database is transcoded into the cultural practice of surveillance in the name of state securitization.² The reduction of the human body into a digital media object becomes most obvious in the binary classifications of "Have a Nice Day" or "Detain for Higher HQ," friend or foe, mobile or immobile, true or false that biometrics ultimately produces.

Visual Typologies and Racial Profiling

The distribution and analysis of the "unidentifiable" terrorist among a large population group in the aftermath of 9/11 relied on the establishment of the typology—or the "generalized look," to go back to

¹ As discussed at length by Allan Sekula and Peter Hutchings, one of the earliest integrations of photography with the science anthropometry took place in the police archive. See Allan Sekula (1986) and Peter J. Hutchings (1997).

² Articulated by Lev Manovich, the term transcoding refers to the translation of computer principles into cultural practices. See Lev Manovich (2001: 47).

Sekula's argument—of the racialized enemy.³ It sought to establish one's true identity through the technological creation of the "terrorist" type out of a biometric automated database. As Kelly Gates has argued, "[l]ike the central role of the archive in the application of photography to criminal identification, the database is at the heart of the biometric system development" (Gates 2011: 102). The digital database-driven "terrorist" type yet again sought to classify the Arab that could be modernized and integrated into the state from the one that should be confined and neutralized. This time however, the process of recognition relied not so much on the scientific expertise of the anthropologist as on the multitude of common soldiers as information-gathers and digital algorithmic logic as data-validator. Computer algorithms based on data gathered in an automated database performed the assessment of one's status. Human Intelligence, I argue, has been profoundly replaced with Automated Intelligence; cultural knowledge has been substituted for mathematic automated calculation of digital data. As I will explicate through the detailing of the specific biometric technologies used in Iraq as described in the *Multi-National Forces West Biometric Standard Operating Procedure* manual from 2007, to which I refer later in the paper, the emergence of the individual human body as a site of veridiction of militarized governmentality is predicated upon the digitization and automation of the indexes as well as logic of the primary regime of truth.

It is important to note that while the racial profile of the "terrorist" in relation to the United States became associated with the general figure of the Arab more specifically, the context of the occupied territory—be it Iraq or Afghanistan—required the computation of the characteristics of the "friendly" Arab. In other words, in the context of a cultural generalization that all Arabs are to be treated with suspicion, automated identification systems promised to signal a "potential friend." Building upon the work of Gates and Richardson, it is the distinction between an Arab foe and an Arab friend rather than the recognition of the figure of the terrorist in relation to the Homeland that this project analyzes through the case study of the biometric endeavors in the 21st century Iraq.

Biometrics in Iraq

Anthropometry reduces the human body to mathematical data to be evaluated through scientific cultural knowledge. Biometrics—the automated recognition of individuals based on measurable biological (anatomical and physiological) and behavioral characteristics—with its reliance on digital recording, storing, and retrieving technologies as exemplified by the digital camera, the digital iris scanner, and the digital database, "transforms the body into a digital media object" to be accessed through computer algorithms (Nakamura 2009: 153-4). While both convert the body into data, biometrics further reconfigures a form of surveillance that no longer has a "primary visual relation" to its subjects but rather functions as "dataveillance"—"a mode of ordering information"—without relying on the act of seeing the body as being of primary importance (Simon 2005: 15). The process of identification is "informed by both acts of seeing and acts of database usage and mechanic data processing: it is both visible and invisible, with the latter tending towards the former in informationalized society" (Nakamura 2009: 154). In the context of the Iraq war, and the War on Terror more broadly, seeing has become a secondary aspect of surveillance. In the biometric database, data is inputted and results are retrieved. It is the database, subjected to the invisible logic of the data processing software, rather than the act of seeing, that determines one's identity and one's relation to the state.

It is the data body, rather than the individual body as invested in a cultural and historical context, that is of interest to contemporary state security practices. As a digital media object, "the individual is doubled as code, as information, or as simulation," effectively transforming him/her into a Deleuzian 'dividual'

³ The racialization of the new "face of terror" in the context of the development of a security and surveillance apparatus within the United States is discussed at length in Kelly Gate's chapter, "Finding the Face of Terror in Data," in *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (2011).

(Simon 2005: 15). Thus in the context of surveillance as *dataveillance*, the body acts primarily as a site of information related to veridiction, rather than verification. *Dataveillance*'s primary interest lies in the establishment of correlations and trends that speak to the security of the state, rather than in the revilement of particular identities. In Iraq, whereas anthropometry at the turn of the century as well as the analog passport were concerned with the establishment of race, tribe, and national origin, biometrics and biometric IDs, rendered indispensable part of the body, served primarily as indicators of one's status as a friend or foe of the nation-state. Anthropometry and analog forms of identification were designed to present a unique identity and further to classify according to multiple typologies such as race, tribe, etc., while computerized biometric identification systems aimed to make a simpler, more dichotomous binary distinction.

The science of biometrics extended the problems of verification and veridiction into a digital rather than analog context (National Science and Technology Council Subcommittee on Biometrics 2006). Biometrics, as Robertson has argued, "is offered as a more reliable set of identification practices, [yet] the claims of reliability are understood within an archival problematization of identity" (Robertson 2009: 331). Biometrics, as means of verification in the broader context of the 20th century, has been deeply dependent upon the creation and maintenance of an archive. The US-driven militarized state-building project for Iraq however deployed biometrics, reliant upon a digital database and the computer logic of true or false, not so much as a technology of *verification*, but rather as a core technology of veridiction. The automated recognition of an individual was meaningful not in terms of the individual's identity, but rather in terms of the individual's security clearance status. As a more sophisticated version of the white headband and the reflective armband described above, biometrics promised the reliable distinction between friend and foe without the burden of becoming familiar with the individual's particular identity.

The biometrics enterprise in 2000s Iraq was driven by the American military. Starting in 2006, the US soldiers became not only gate-keepers and state-builders of the Iraqi state, but also data collectors armed with a rifle in one hand and a computerized recognition device in the other. Lacking cultural and historical knowledge of the region, they relied on automated technology that took fingerprints, iris scans, and facial recognition photographs in determining who can be a potential Iraqi ally and who has been and will remain a foe, targeting particularly "men of fighting age" (Shanker 2011). The focus of the biometric enterprise on Iraqi men aged 15-64, signals the racial and gender parameters that have constructed the supposedly neutral digital computerized body template. The secondary place relegated to women and children also speaks to the emphasis on securitization in terms of a dual friend/foe understanding, thus a process of veridiction, rather than massive comprehensive identification, or verification.

In the case of the town of Fallujah, the military evacuated all of the men, women, and children and allowed them to return to their homes after they had been enrolled into a biometric database (Homeland Security News Wire 2009). The case-study of Fallujah is a prime example of the totality that the biometric projects seeks. As Benjamin Muller has eloquently argued, this failed enterprise attempted to purge Iraqis out of their old identities, based on "family, language, architecture...familial, clan, or tribal bonds" and enforce a "new, biometrically catalogued and determined identity" (Muller 2010: 114). It makes one wonder whether, given the opportunity, in an ideal securitization scenario the entire Iraqi nation would be evacuated from the state, registered in a biometric database, and then only the good guys would be let in! The *society of total control* actualized.

The "securitization" of the country was dependent on the successful control of movement of people, which in turn was enacted through a massive-scale, computerized mobile surveillance. Biometrics was deployed for "offensive purposes as an integral tool in military operations, as opposed to just a defensive system for military installations" (Biometrics Identity Management 2007). Checks were to be performed not only at the border but more profoundly throughout the territory by hand-held mobile devices. A five second computer scan of either one's iris or one's biometric badge can determine, based on the visual

message displayed, whether one can go ahead and “Have a nice day” or will be detained and tortured. Individuals are entered into a database and given an “ALERT” status.

By the end of the American militarized state-building mission in Iraq in 2010, close to three million Iraqis, mostly men between the ages of 15 and 64, were enrolled into a biometric database. Among those recorded in the 2003-10 biometric enterprise were potential employees for Iraqi security forces, contractors at the US military bases, students, tribal and local officials, criminals, insurgents, detainees, as well as ordinary individuals that inhabited an area that was being “secured”—civilian men, as well as women, and children. In some instances, entire villages were evacuated and all of the men, women, and children that inhabited a particular territory were entered into a biometric database before they were allowed to return (Homeland Security News Wire 2009).

Figure 1: Biometrics on the ground and in the DOD
A Soldier uses the Hand Held Interagency Identify Detection Equipment System to fingerprint and photograph new Iraqi police recruits at the IP Academy in Mahmudiyah, Iraq. Image Courtesy of www.army.mil (<http://www.army.mil/article/21940/biometrics-on-the-ground-and-in-the-dod/>)

The stationary Biometric Automated Toolset (BAT), deployed in 2003-2010 US-led occupation of Iraq as well as in Afghanistan, combines visualization hardware (fingerprint reader, iris scanner, digital camera) with a complex database in order to collect and compare “fingerprints, iris images, and facial photos” (Biometrics Identity Management 2010) (see Figure 1). A total of two iris scans, one photograph, 10 fingerprints, and 34 items of biographic information (including interrogation reports) are gathered for each individual in order to control the movement of individuals across the Iraqi border, the US bases, as well as in the larger territory of the Iraqi state (Biometrics Identity Management 2010; Lambert 2010).

All of that information was then used to create a robust database as well as individual personal badges to be worn by the “enrolled” Iraqi population. One Iraqi after another is asked their name, their tribe, and told to put their fingers on the glowing green scanner (Shachtman 2007). One’s identity thus was initially captured in the biometric enrolment process and subsequently reconfirmed from a badge. The badge provided a “barcode” and a “number” which could not be falsified and can be in turn used by the military to “screen the individual and determine ‘Go’ or ‘No Go’ in less than 5 seconds” (MNF-W 2007: 13). The photograph, biographic, and physical information help to verify the identity of the individual in question. This identity is useful however mostly in determining a friend or foe status, rather than for gaining

knowledge about racial, tribal, or criminal cultural and physiological traits. Muller has critically argued that under the biopolitical biometric state “cultural investment” and respect for “local knowledge” become irrelevant: “the Other is simply reconstituted through biometric applications into the suspect identity” (Muller 2010: 110).

The control of the Iraqi population was enacted not only at the entry points of “secured” encampments such as the “Green Zone” but also across the general territory of the Iraqi state. Biometrics was no longer a solely stationary enterprise. It has become mobile. The mobile version of BAT used in Iraq and Afghanistan is called Handheld Interagency Identity Detection Equipment (HIIDE) and captures fingerprints, iris scans, facial photographs, and biographical information (Biometrics Task Force 2007). This system was first introduced in Iraq in 2006 and quickly became a “workhorse handheld capability” (Fenton 2008). The system enables soldiers to take the biometric information of individuals they encounter while on patrol.

In short, the biometric project for Iraq during the 2003-2010 Iraq War relied heavily on the use of digital automated technologies both for its data collection as well as for its data analysis. Whereas anthropometry relied on scientific knowledge of culture for the interpretation of the gathered data, biometrics replaced this knowledge with computer-driven algorithmic processes. Further, it radically transformed the meaning of the analysis produced. In answering the question “Who are you?,” biometrics in Iraq provided a binary solution: a friend that can “Go,” or a foe that is a “No Go.” The individual body thus became a site of veridiction rooted in the notion of motion and confinement not within the penal system itself, but rather within the state more broadly. It provided a regime of truth directly linked to militarized governmentality, a governmentality in which the penal logic is the prevalent logic of governmental securitization process.

Scientific Expertise, Automated Intelligence

The process of automation and digitization of biometric technology has replaced the science expert with the common user. Soldiers, trained to use the biometric technology but not versed in the sciences of biometrics and even anthropology, sociology or history, can now capture information and identify strangers with little training and expertise. “Like technology from the latest spy movie, a system using finger prints and retina scans helps soldiers tell the difference between the good guys and the bad guys in Iraq” claims an article posted on the official US Army website (Cooper 2010).

Scientific cultural knowledge, and more specifically anthropological knowledge, figures only marginally in the biometric project in Iraq even though it has been foundational for the establishment of the anthropometric and biometric apparatuses in the past. In 2010, Army Lt. Col. Kimberly Johaneck, an adjunct professor of Sociology at Boise State University and head of the RAOC (Rear Area Operations Center) Badging Office, was responsible for the biometric security badges that control access to the Green Zone in Baghdad and in 2010 was “trying to encourage the Iraqis to use biometrics, which match fingerprints or iris scans against a database” (Spinner 2011). Most of the active biometric data-gathering and people-sorting however is done by soldiers who have completed a weeklong technology crash course and have no background in scientific social knowledge (Greene 2012) even though I think that they should.

The US military in 2003-10 was equipped with high-tech digital identification devices that automated the process of identification and authentication, effectively removing the need for scientific or cultural knowledge in the process of recognition (see Figure 1). Classification of bodily features became irrelevant as “Iris Technology” now examines 266 unique spots of the iris mapping them onto a digital template called “IrisCodeT” (Kaucher n.d.). All of this detailed information however did not lead to complex racial classificatory schemas, but rather to a simple 4-pronged menu that was further reduced to a “Go” or “No Go” scenario:

He's an Iraqi bad guy (in reality Former Regime, Detainee, AQIZ, 1920 etc.)
He's an 'external' bad guy (foreign fighter)
He is a low-level criminal.
He is a local citizen.

(WNF-W 2007: 11)

The new biometric technology did not aim to foster any understanding of the racial or cultural background of the subject. Biometrics here is quite divorced from cultural anthropology. Instead, it is concerned only with answering the question: "are you a foe and if so what kind?"

Indeed, "[t]he technology promised success where human security staffers failed, compensating for their imperfect, subjective perceptual abilities and limited memory capacities" (Gates 2011: 101). This quote offers a particularly striking comparison between the capabilities of a human and a computer to distinguish a friend from foe. "Human security staffers" fail because of insufficient technological parameters. Their intelligence and aptitude is measured by their "limited memory capacity"—the brain of a staffer offers less operating memory than the biometric HIIDE device: the former could never store and retrieve 22,000 full biometric profiles, the latter does this in a matter of seconds. Human visual perception is also questioned, as the naked eye cannot discern 266 unique spots of the iris. In summary, during the 2003-2010 high-tech Iraq War technology was seen as the advanced and more accurate substitute for cultural awareness in the context of militarized state-building through securitization. The veridiction of the US-led militarized governmentality in Iraq was entrusted in the computer algorithm rather than in the scientific knowledge.

Immobilized Foe, Secure State

The securitization of the Iraqi state during the Iraq War relied heavily on the control of "flow" and "traffic." As Lieutenant Colonel Jeff Smitherman, head of the biometric badging program for Multi-National Forces-West in Al-Anbar province, has said: in the Iraq War 2003-2010, biometrics have been used predominantly to deny insurgents "freedom of movement" (Shachtman 2007). Biometric badging, coupled with mobile biometric scanners, in contrast to the traditional passport and stationary border check-point system, promised to deliver the latest and most reliable method of veridiction for "Population Control" purposes by restricting the movement of those deemed to present danger to the state (MNF-W 2007: 12).

The securitization logic of controlling movement within and across the borders of the uncivilized state relies on the visualization and isolation of danger. The identification and quarantine of the foe in the 2003-2010 militarized state-building enterprise in Iraq happened not only at the border check-points but within the territory of the state itself. The American military was transformed literally into an army of mobile biometric data-gatherers. It became a mobile unit aiming to control the movement of people within the Iraqi nation (Cooper 2010). This "herculean" collection effort is fueled by the proliferation of mobile biometric technology (Fenton 2008). The biometric securitization effort in Iraq included people moving either by foot or motorized vehicle on the street and was in turn conducted by a highly mobile and quite numerous military. The preoccupation with movement is also evident in the explicit naming of "taxi or truck drivers" as a category of people that should be captured in the biometric database (MNF-W 2007: 13). Biometric research moved away from the centralized confines of the camp, prison, or hospital and away from the border points on the periphery into the core of the nation. A highly movable unknown foe required a highly mobile easy-to-use automated dispersed biometric system.

Biometric badging, coupled with mobile biometric scanners, in contrast to the traditional passport and stationary border check-point system, promised to deliver the latest and most reliable method of veridiction for "Population Control" purposes by restricting the movement of those deemed to present

danger to the state (MNF-W 2007: 12). Whereas 20th century anthropometric research and government identification initiatives produced identification documents as well as the typological schemas that functioned as a “technology of verification,” during the Iraq War biometric research and militarized governmental identification practices aimed to distil in simplistic terms Arab foes from Arab friends (Robertson 2004: 454).

Conclusion

The distinction of allies and enemies during the Iraq War was further articulated by the logic of digital technologies. The US military gathered biometric data through high-tech devices and produced simplistic binary labeling of “friends” and “foes.” Data was compiled into a digital database that in and of itself obscures data. Furthermore, the process of classification that anthropometrics utilized relied on highly specialized scientific knowledge, while in the context of contemporary digital biometrics, it was subjected to an automated computer algorithm. Despite these differences, the US military biometric project extends the logic of securitization of the state. “Who are you?” remained a central question to be asked of each member of the Iraqi state in both instances of militarized state-building. The American-led administration of Iraq, however, was happy with a dichotomous answer generated by automated intelligence distinguishing the true friend of the state from the impostor who must be detained and thus neutralized.

References

- Acherman, Spender. 2011. U.S. Holds on to Biometrics Data from 3 Million Iraqis. *Wired.com*. December 21, 2011. <http://www.wired.com/dangerroom/2011/12/iraq-biometrics-database>. (Accessed May 27, 2012).
- Altwood, Brian. 1994. Suddenly, Chaos. *The Washington Post*. July 31, 1994, p C9.
- Biometrics Identity Management Agency. 2010. *Biometric Glossary Version 5*. <http://www.biometrics.mil/Files/Documents/Standards/BioGlossary.pdf> (Accessed May 22, 2012).
- Biometrics Task Force. 2007. *Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE)*. September 19, 2007. http://biometrics.nist.gov/cs_links/standard/archived/workshops/xmlandmobileidPresentations-docs/Vermury-BAT-HIIDE.pdf (Accessed May 22, 2012).
- Cooper, Chad. 2010. BATS helps ID insurgents, hostages. *The official website of the United States Army*. January 7, 2010. <http://www.army.mil/article/32609> (Accessed May 21, 2012).
- Cordesman, Anthony and Emma Davies. 2008. *Iraq's Insurgency and the Road to Civil Conflict* Vol 2. Westport, CT: Praeger Security International.
- Deleuze, Gilles. 1992. Postscript on Societies of Control. *October* 59: 3-7.
- Fenton, James. 2008. HIIDE Gets an Update: New Software Adds Storage Capacity and More. *The Biometric Scan*. October 4(4). http://www.biometrics.dod.mil/Newsletter/issues/2008/Oct/v4issue4_pm.html (Accessed May 22, 2012).
- Foucault, Michel. 1969. *Archaeology of Knowledge*. New York: Pantheon.
- Foucault, Michel. 1995. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.
- Foucault, Michel. 2008. *The Birth of Biopolitics*. Michel Senellart, ed. Graham Burchell, trans. Basingstoke [England]; New York: Palgrave Macmillan.
- Gates, Kelly. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York and London: New York University Press.
- Greene, Antonia. 2012. Including biometrics in deployment training helps Soldiers identify the enemy. *The official homepage of the United States Army*. April 30, 2012. http://www.army.mil/article/78894/Including_biometrics_in_deployment_training_helps_Soldiers_identify_the_enemy/ (Accessed August 4, 2012).
- Homeland Security News Wire. 2009. Worries about Iraq's biometric database. *Homeland Security News Wire* August 26, 2009. <http://www.homelandsecuritynewswire.com/worries-about-iraqs-biometric-database> (Accessed June 12, 2012).
- Hutchings, Peter J. 1997. Modern Forensics: Photography and Other Suspects. *Cardozo Studies in Law and Literature* 9 (2): 229-243.
- Kaucher, Peter. n.d. “Iris Technology” Biometrics 101: A Little Science *Biometric Identity Management Agency*. <http://www.biometrics.dod.mil/References/Tutorial/8.aspx> (Accessed June 7, 2012).
- Lambert, Delle. 2010. Biometric assignment in Iraq results in dramatic job focus for major. *The official homepage of the United States Army*. February 26, 2010. <http://www.army.mil/article/35082> (Accessed May 22, 2012).
- Locy, Tony. 2003. Military lawyers begin sorting out Iraqi prisoners, deciding their fates. *USA Today*. April 10, 2003, 5A.
- Manovich, Lev. 2001. *The Language of New Media*. MIT Press: Cambridge MA and London England.
- Muller, Benjamin. 2010. *Security, Risk, and the Biometric State*. London and New York: Routledge.

- MNF-W Biometric SOP (Multi-National Forces West Biometric Standard Operating Procedure) Operation Iraqi Freedom Version 1 2007. <http://info.publicintelligence.net/MNF-W-HIIDE-SOP.pdf> (Accessed June 11, 2012).
- Nakamura, Lisa. 2009. The socioalgorithmics of race: sorting it out in Jihad worlds. In: *The New Media of Surveillance*, eds Shoshana Magnet and Kelly Gates, 149-162. London and New York: Routledge.
- National Science and Technology Council Subcommittee on Biometrics. 2006. *Biometric Glossary*. September 14, 2006. <http://www.biometrics.gov/Documents/glossary.pdf> (Accessed July 10, 2012).
- Partlow, Joshua. 2007. For U.S. Unit in Baghdad, An Alliance of Last Resort. *The Washington Post*. Saturday, June 9, 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/06/08/AR2007060802879.html> (Accessed June 7, 2012).
- Poster, Mark. 1990. *The Mode of Information: Poststructuralism and Social Context*. Chicago: The University of Chicago Press.
- Poster, Mark. 1996. Database as Discourse; or Electronic Interpellations. In: *Computers, Surveillance, and Privacy*, eds David Lyon and Elia Zureik. Minneapolis and London: Minneapolis University Press.
- Pugliese, Joseph. 2010. *Biometrics: Bodies, Technologies, Biopolitics*. New York and London: Routledge.
- Robertson, Craig. 2004. The Archive, Disciplinaryity, and Governing: Cultural Studies and the Writing of History. *Cultural Studies<->Critical Methodologies* 4(4): 450-471.
- Robertson, Craig. 2009. A Documentary Regime of Verification: The Emergence of the US passport and the archival problematization of identity. *Cultural Studies<->Critical Methodologies* 23(3): 329-354.
- Sekula, Allan. 1986. The Body and the Archive. *October* 39: 3-64.
- Shanker, Thom. 2011. To Track Militants, U.S. Has a System That Never Forgets a Face. *New York Times*. July 13, 2011. <http://www.nytimes.com/2011/07/14/world/asia/14identity.html> (Accessed October 13, 2013).
- Shachtman, Noah. 2007. Iraqi Diary: Fallujah's Biometric Gates (Updated) *Wired.com*. August 31, 2007. <http://www.wired.com/dangerroom/2007/08/fallujah-pics> (Accessed May 21, 2012).
- Simon, Bart. 2005. The Return of Panopticism: Supervision, Subjection, and the New Surveillance. *Surveillance & Society* 3(1): 1-20.
- Spinner, Jackie. 2011. Badge Wars: The woman who controls access to Baghdad's Green Zone is one of the most powerful Americans in Iraq. *Slate*. May 10, 2011. http://www.slate.com/articles/news_and_politics/dispatches/2011/05/badge_wars.html (Accessed August 4, 2012).
- Stockman, Farah. 2010. Worries about US data on Iraqis: Privacy advocates, those scanned fear misuse if files shared. *Boston.com*. August 31, 2010. http://www.boston.com/news/nation/washington/articles/2010/08/31/questions_arise_about_use_of_data_gathered_in_iraq_war (Accessed June 11, 2012).