Grey's Anatomy goes South: Global Racism and Suspect Identities in the Colonial Present

Colleen D. Bell

Abstract. This article explores the biometric documentation of civilians by coalition forces in the battle zones of the "war on terror." With the growth of population-centric operations, harvesting body data is a key dimension of efforts to divide the population between civilians and insurgents, and also serves as a general strategy of population management over life perceived to be potentially dangerous. This article examines how these dividing and governance tactics are part of a global racism that is manifest in North-South conflict. The racism that underpins biometric technology is reflected in the racial dynamic of Western-led counter-insurgency operations, in which the US and its allies expand control over southern populations. In so doing, the insecurity of said populations is deepened and the political dimensions of global inequality are accentuated.
Keywords: biometrics, race, racism, counterinsurgency, war on terror, biopolitics

Résumé. Cet article examine la documentation biométrique de civiles par les forces de coalition dans les zones de bataille de la "guerre contre la terreur." Avec la croissance des opérations centrée sur la population, la récolte des données du corps est une dimension essentielle des efforts déployés pour diviser la population entre les civiles et les insurgés, servant aussi comme une stratégie générale de gestion de la population contre la vie perçue comme potentiellement dangereuse. Cet article examine comment ces tactiques de division et de gouvernance font partie d'un racisme global qui se manifeste dans un conflit Nord-Sud. Le racisme qui soutient la technologie biométrique est reflété dans la dynamique raciale des opérations anti-insurrectionnelles menées par l'Ouest, dont les États-Unis et ses alliés étendent le contrôle sur les populations du Sud. Ce faisant, l'insécurité de ces populations est s'approfondit et les dimensions politiques des inégalités dans le monde sont accentuées.
Mots clés: biométrie, racé, racisme, contre-insurrection, guerre contre le terrorisme, biopolitique

> *“‘Like Mao said, insurgents are like fish swimming in the sea of the people.’ These are the high-tech nets, to keep ’em from swimming freely’.” Lieutenant Colonel Jeff Smitherman (Shatchman 2007a).*

In a converted school house in Fallujah in early 2005 US Marines began a program of biometric data collection of Iraqi civilians. The program was erected in the aftermath of the second major battle of Fallujah in which elements of the civilian population (rather than Baathist forces) organized a rebellion against the US invasion. During the conflict upwards of 200,000 people were evicted from the city. The conditions set by the coalition for people’s return required that they submit to a biometric badge containing digital fingerprints and an iris scan. By 2007 the program had become mundane, with traffic trickling in like that of a passport office in a small town. A reporter from the data collection site noted that the half dozen Marines operating the program seemed bored beyond words: “they blast Three-Six Mafia and watch videos on their laptops to keep from climbing the walls” (Shachtman 2007a). One Marine used his post as an opportunity to catch up on episodes of *Grey’s Anatomy* presumably missed while he was busy fighting more kinetic battles elsewhere.

Inadvertently, *Grey’s Anatomy* carries a separate significance in this context. Growing biometrics in the battlezones of the “war on terror” are one aspect of a strategy to divide the population into friends and enemies. In fact, the US military approaches the populations that it confronts according to a conceptual grid of “blue,” “grey,” and “red” people. The so called “blue” folks are perceived to be friendly while the “red” people are determined to be hostile insurgents. The position of the “grey” people is uncertain. These days, uncertainty is frequently aligned with threat, and concerted action on such grounds is easily compelled. A system that claims to unearth the biometric composition of a population is designed precisely to offer a new scope of visibility. It is to determine “the probability of whether a grey category person falls into the blue or red category” (Gold 2010:8; also see Woodward 2005). Hence, determining greys’ anatomy, in both biological and political terms, has become a vital maneuver in fighting wars amongst the people.

In contrast to this search to authenticate the anatomy of grey, Donna Haraway (1991) once noted that visibility is always constructed. What we see is always provisional, partial, and culturally produced. Though visibility is about rendering “other spaces” transparent, since it is constructed, it always creates spaces of invisibility. Digital biometric technology represents a striking manifestation of this apparent paradox. Rather than simply revealing the authentic “truth” of the body, the science that underpins it reproduces hegemonic stereotypes and targets vulnerable and racialized populations (Pugliese 2007; Magnet 2011). On the global scene, biometric technology is deployed as a tool for counterinsurgency which claims to expose the insurgents that hide among the population. Yet, it seems to produce the opposite of what it envisages. Rather than simply extracting the “enemy,” biometric technology casts whole populations as potential enemies, thereby enhancing local insecurity and possibly encouraging insurgency.

This article explores the biometric documentation of civilians by coalition forces in the battle zones of the “war on terror.” Mission setbacks in the US-led interventions in Iraq and Afghanistan have led to a growth in population-centric operations. While cultural programming, such as the human terrain program, has received critical attention (Kelly et al. 2010; Bell 2011; Ansorge 2010), less has been said about US efforts to capture the biological identities of Iraqi and Afghan peoples. The US military regards biometric technology as a “game changer” and as an “operations weapons system” (Biometrics Identity Management Agency [BIMA] 2012). Harvesting body data is a key dimension of efforts to divide the population between civilians and insurgents, while also serving as a general strategy of population management over life perceived to be potentially dangerous. This article examines how these dividing and governance tactics are part of a global racism that is manifest in North-South conflict (Barkawi and Laffey 2006). It argues that the racial history and racism of biometric technology is reflected in the racial dynamic of Western-led counterinsurgency operations, in which the US and its allies expand control over southern populations. In so doing, the insecurity of said populations is deepened and the political dimensions of global inequality are accentuated.

The article first discusses aspects of biometric security operations in Iraq and Afghanistan. Second, it reviews the ways in which biometric science is shaped by biological essentialism and stereotypes, while also highlighting the way in which racialized populations and populations perceived as deviant have long been the targets of biometrics. Ironically, however, the technology struggles to account for bodies that are non-white and to function in environments that are “uncontrollable.” Third, the discussion connects biometric operations to broader dynamics of the colonial present to illustrate the way in which the technology reproduces colonial North/South relations. Military biometrics, involving the involuntary seizure of the body data of foreign, occupied populations, accentuate global inequality and racism. On the basis of suspicion and preemption, they lead to a tightening of control over global circulation by the US and its allies, and the subordination of the rights, safety, and autonomy of Iraqi and Afghan civilians. These dynamics are taken one step further in the fourth section where I place the experimental status of military biometrics within the legacy of the colonial laboratory. I conclude that despite the remarkable investment and growth of the biometric industry, it is not without its failures and weakness. In particular, the application of biometrics in Iraq and Afghanistan treats whole populations as suspect and expresses radical fear and estrangement from the very people that counterinsurgency claims to protect.

By design, biometric technologies categorize people, distinguishing between deserving/undeserving, safe/threat, high risk/low risk and so on. One important prerequisite for the success of this kind of categorization is the enrollment of as many identities as possible. Hence, a good starting point for making sense of these dividing practices is Zygmunt Bauman's (1989) argument that a distinguishing feature of racism is the quest to produce and institutionalize a stringent social order. Racism follows the patterns of medicine and gardening in which the objective is always to separate and set apart "the useful elements designed to live and thrive, from harmful and morbid ones which ought to be exterminated" (1989:70). In other words, racism involves the extermination of undesirables alongside the incorporation of those lives which are desirable. This relation resonates with a biopolitical understanding of racism as "the break between what must live and what must die" (Foucault 2003b:254–55). Such a break requires separating out groups within a population and casting war in biological terms in which the death of the other corresponds directly to the life of the self. Thinking about racism in biopolitical terms is a way of capturing the double movement of a politics that takes hold of life while also enacting death. By this regime of power, everyone is categorized, no one is exempt. Focused around identification and verification, for the purposes of authorization and exclusion, biometric technology is a means of institutionalizing a discriminatory ethic. Its expansion into war zones enhances not only the exclusionary, but also exterminatory, potential of racism.

Biometrics in the War on Terror

In times of war and crisis surveillance regimes often undergo expansion and development (Aas 2006). Seizing the biometric data of citizens, residents, and visitors in various programs that link mobility to national security is generally understood to be a signature feature of Western post-September 11, 2001 surveillance regimes. Such technology is perceived, especially by its proponents, to be the frontline of securing borders from unauthorized migrants and potential terrorists. Certainly, the technique of measuring and analyzing biological data for the purposes of identification and authentication has been around for centuries (Maguire 2009). Modern developments in biometric technology in the 1980s and 90s, concerned primarily with controlling prison populations and welfare recipients, proved to be costly and incompetent. The terrorist attacks of 2001 have been credited with pushing the biometric industry into stable profitability (Magnet 2011:164). With the export of biometrics to document the populations of Iraq and Afghanistan, the biometric industry has widened its market.

According to the supply company Northrop Gurmman, the biggest user of biometric technologies next to the US Department of Homeland Security is the Department of Defence. Currently the US military, the UK Ministry of Defence, and NATO are all using biometric technology in their missions. Thousands of portable iris recognition and enrollment devices are in operation in Afghanistan, Iraq, and Bosnia (Fordyce 2007; L-1 Identity Solutions 2007). For example, Homeland Security, alongside NATO and the Afghan government, worked to issue biometric ID cards to 1.6 million Afghans between 2010–2011. The stated goal was force protection and anti-infiltration. The movement of suspicious people is monitored and data profiles are cross-referenced with other biometric databases that have been up and running for some time to catch "Taliban infiltrators" attempting to join the Afghan army. It has been boasted that the program catches 20–25 people per week who would have gone undetected by conventional methods (Gold 2010:7). These results are attributed to not one but two active programs in the country. The first, named the Biometric Automated Toolset (BAT), generated more than 400,000 data sets of detained individuals and persons of interest by the end of 2010, after only 18 months in operation. The second — Afghan Automated Biometric Identification System (AABIS) — collects data from police and army applicants. Pioneered by NATO and Homeland Security "in close cooperation with the Afghan National Army," the data "is cross-matched with the databases operated by the Afghan National Detention Facility, the Kabul Central Police Command, the Counternarcotics Police of Afghanistan and FBI prison enrollments from Kabul, Herat and Kandahar" (Gold 2010:7). By late 2010 AABIS had accumulated 248,768 data sets and thousands more are being recruited to resurrect Afghanistan's national ID program (Shachtman 2010:2; Nordland 2011). As of 2012, the program scanned more than 2.5 million Afghans (*Economist* 2012).

The resurrection of the national ID system is an about-face for President Karzai who, in the summer of 2010, shut down the NATO supervised program for a time. Citing concerns over Afghan sovereignty, Karzai's actions followed *Newsweek*'s photo coverage of biometric checkpoints in Kandahar city. The system was modeled on the walling of Fallujah at the height of the Iraqi insurgency (Shachtman 2010:3). Indeed, while biometric sweeps in Afghanistan are unprecedented and recent, coalition programs in Iraq began in 2004 and have been built on top of databases assembled during the reign of Saddam Hussein. Only a year into the war, the US military installed "more than 100 iris scanners and fingerprint checkers" in Iraq (Shachtman 2007b). Also, prior to the walling of Fallujah, US troops sought to reclaim the city of Baqubah and capture and kill the 300–500 insurgents believed to be housed there by seizing the biometric footprint of "every resident who seems to be [a] potential fighter" (Shachtman 2007b).

Though it is difficult to ascertain precisely how many people in Iraq and Afghanistan have had their biometric data harvested, it is clear that there is a systematic effort to document as many people as resources will allow (Nordland 2011). That is, though the biometric data collection is explained as a key means of catching and intercepting insurgents, the efficacy of the technology is reliant on data mining mass society. It is consistent with the general strategy, outlined at the outset of this article, to categorize the population and determine the status of the "grey" unknowns. As an aggregative strategy to acquire intimate knowledge of population, biometrics are an outgrowth of biopolitical rationalities of power (Pugliese 2010:46). In fact, the use of body data highlights the biopolitical principles of counterinsurgency in which occupying states seek to not merely extinguish insurgency, but to take hold of the life of the population towards such ends. Indeed, a key, classical, feature of counterinsurgency is the collection and aggregation of population data. As the counterinsurgency guru David Galula noted, "control of the population begins obviously with a thorough census … every inhabitant must be registered and given a fool proof identity" (2006:84). This strategy fits contemporary "best practices" of counterinsurgency, which recall how British successes during the Malay Emergency rested on the issuance of ID cards with photo and fingerprint to the population (Sepp 2004:10). Following this recommendation, checkpoints established by the US military were erected to compile a census of 10 of Baghdad's most violent neighbourhoods (Niva 2008:74; Kingsbury 2008). The task was performed by scanning the irises and fingerprints of residents, to establish administrative, biopolitical, control over the population. Before moving to examine the global politics at play when foreign, occupying, militaries collect the biometric data of conflict-affected populations, the discussion will first address the more immediate relationship between racism and biometric science, revealing additional sites of overlap between biopolitical rationality and counterinsurgency.

Biometric Science and Racism

Biometric technology claims to offer a culturally neutral means of capturing and authenticating the physical and behavioural characteristics of individuals to verify identity. There are a range of devices that scan palm or finger prints, facial structure, iris patterns, and, most recently, gait. The management, interdiction, and categorization of suspect identities have always been key objectives of biometric technologies. These fundamental purposes are deeply racialized and gendered. As Joseph Pugliese has demonstrated, biometric technologies are imbued with "infrastructural relations of disciplinary power underpinned by normative categories of race, gender, (dis)ability, sexuality, class, and age" (2010:2). However, the official story of biometrics claims otherwise. Routinely such technologies are touted as objective, neutral, instruments of security. Biometrics are claimed to be "racially blind" technologies capable of overcoming discriminatory security regimes. Yet given that computers are not actually capable of seeing faces, argues Kelly Gates (2011), there is no culturally neutral means of visual profiling. In addition, biometrics are fundamentally premised on the idea that human beings have consistent, heritable characteristics that can be discovered, aggregated, and acted upon. The word "biometrics" is derived from *bios* and *metron* which "denotes the recognizing of humans on the basis of intrinsic physical or behavioural characteristics" (Maguire 2009:9). The science upon which it is constructed presumes that the body is a "stable, unchanging repository of personal information from which we can collect data" (Magnet 2011:2).

Correspondingly, the field of biometrics has sought to breathe new life into formally debunked forms of scientific inquiry, such as physiognomy and anthropometry, that are rooted in biological understandings of gender and race. Biometrics have a prehistory of proto-technologies focused on identifying, measuring, and classifying the body and behaviour (Pugliese 2010:25–55). Despite documented failures of these studies, and the technologies derived from them, biometric science has contributed to attempts to normalize the most hegemonic, stereotypical, understandings of gender and race. In the face of burgeoning research on the complexity of identity and the social construction of race and gender, the biometric industry has played a significant role in the resurrection of biological theories of race and gender. In addition, these very normative and discredited understandings of race and gender are inescapably coded into the technologies themselves (Gates 2011). Biometrics are not only based upon debunked science, but have been developed and nurtured in a cultural context in which biometric scientists must decide, themselves, on the boundaries and classifications of racial and gendered "markers" (Magnet 2011).

These circumstances cannot be separated from the communities that have long been the targets of biometric technologies. Widespread in North America and Europe, prison populations, as well as welfare recipients, have been required to submit to biometrics. These populations are also overwhelming from racialized communities. Despite being forced on racialized populations (in contrast to the opt-in programs now available to affluent travelers), biometric technologies assume whiteness (Pugliese 2007). The bodies imagined by biometric technologies are light-skinned and light-eye coloured. For example, biometric technology has consistently failed to capture the digital fingerprints of Asian women and has repeatedly failed to scan dark toned irises because it cannot differentiate the irises from the pupils (Magnet 2011:25–29). The technology is confounded in attempts to document peoples who defy normative gender representations of masculinity and femininity. It also has consistently failed to acquire the data of visually impaired peoples, for example, those with cataracts which, as the United Nations Human Rights Council (UNHRC) discovered in its biometric program for aid recipients, afflicts a high proportion of the Afghan population and the region more generally (Jacobsen 2010:93). The functional ability of the technology presumes "ideal conditions" in which illumination, heat, and dust levels can be controlled and adjusted, in remarkable contrast to the rugged landscapes of military and humanitarian operations (see Evans 2012). In other words, the ideal subject, structurally built into biometric technology, is white, pale-eyed, probably male or stereotypically masculine, able-bodied, living in an affluent control society. As Pugliese argues, biometrics may ask the question "who are you," but the answer to this question is largely determined by the prior question of the embodied, geopolitical status that circumscribes "what you are" (2010:1). What we have, thus, is a technology that is both racializing in its application, and structured on the normalization of whiteness. This is precisely the circumstance in which racialized bodies experience what Franz Fanon called "being through others" (1967:111). Though used consistently to govern racialized populations, biometric technology is a form of "digital epidermalization" rendering certain bodies "out of place" (Browne 2010:134).

With the scientific underpinnings of biometrics in question, it is important to consider the assumptions that inform the use of this technology in conflict settings. In the first place there is an assumption that insecurity and invisibility are connected. Enrollment of people in the database is, correspondingly, thought to render those identities secure or "known" (Muller 2010:101) In short, identities that are simply unfamiliar are immediately associated — *on the basis of their unfamiliarity* — with insecurity and danger. Another assumption is that the technology is capable of easing the difficult task of fighting insurgency in a foreign context. Though the US military has put resources into cultural awareness programming in operations in Afghanistan and Iraq, the use of biometrics is thought to be a potential shortcut to the same goal. In the face of complex encounters with local leaders and customs, biometric technology promises to circumvent the need for genuine "face to face encounters" and to "solve the current problem of matching spelling of local names" (Muller 2010:110; Prickett 2005). Learning the complexity of local identities is a long-term endeavour, whereas the BAT system can be mastered in a couple of days. In the purportedly simpler route of biometric enrollment, notes Muller, "the other is simply reconstituted through biometric applications into a suspect identity" (2010:110). The deployment of technological rationalism imposes singular identities in the place of actually dealing with "social history and semantic meaning" (Homs 2008:88).

For the US authorities in Iraq, imposing a singular identity was precisely the means through which to undermine the complex cultural and political networks of Fallujan identity. For the counterinsurgency to gain ground, the very things which provided Fallujans with a sense of place and solidarity — "the connections between local affinity groups and familial bonds and the linguistic and other identity markers" — had to be displaced (Muller 2010:114). New identities constructed through foreign logistics involved the systemic division of Fallujans into new categories required to highlight post-Saddam Iraq. People could thus be slotted into the category of "new Iraqis" thought to be mainly composed of women, children, and the elderly, while those perceived or known to be Baathists, insurgents, or worse, Jihadis, were the "old Iraqis" that threatened the new order. To recall the earlier taxonomy of counterinsurgency, the anatomy of the "greys" in this fantasy represents the undecidable, suspect, category of noncombatant adult males aged 15–45, whose allegiance to the new order is questioned. In Afghanistan today, a similar classification regime is in place, in which scanning males between the ages of 15–70 is compulsory (*Economist* 2012).

Assumptions about the power of biometric scanning in conflict settings suggests that the racial politics of biometrics are geopolitical (in addition to scientific and technological). For some time, US ports-of-entry have been relocated within the borders of other nations. However, the extension of biometrics at issue here is among populations who have not necessarily made requests to travel to the US or an allied nation (or only do so later). Most are seeking employment, or are internally displaced and attempting to return to their country or community. To qualify as humanitarian subjects, Afghans and Iraqis must be catalogued and validated (as neither terrorists or insurgents) within an emerging regime of global identity control by the US and its allies (Schwartz-Dupre 2007:441). In this respect, the biometric documentation of war-affected populations represents an emerging security technology that extends the policing of global circulation.

Circulation and Control in the Colonial Present

According to Sun Tzu, war is best waged by other means. To defeat one's enemy without violence is the "acme of skill" (1971:Chapter IV). The modern spin on this strategy of war by other means is reflected in key shifts in command and control on the battlefield in which computers and digital technology, intelligence, as well as culturally sensitive communications have become "force multipliers" (Petraeus 2006:3). Indeed, information technology has provided the means by which "full spectrum dominance" supplants discrete battlefields (Der Derian 2003:453). And yet, despite the futuristic orientation attached to such technologies, Derek Gregory (2004) has described the ongoing wars on terror in Iraq, Afghanistan, and Palestine as indicative of the "colonial present." To understand the dynamics of modern warfare we must rethink "lazy" separations between the past, present, and future and come to terms with the colonial currents shaping modern conflict (see, for example, Fontan 2006).

The biopolitical power of biometrics is a key connection between the colonial past and the colonial present. As Patel and McMichael (2004) have shown, colonial government was, in essence, about the management and control of bodies. Instrumental to the establishment of colonial rule in the 19th century was the induction of non-Western subjects into biopolitical programs of measurement "designed to regulate, administer and hierarchise" (Pugliese 2010:42). Local populations were routinely required to

> cover their bodies, subject their bodies to hygiene, fill their bodies with Western knowledge, move their bodies to different lands, use their bodies for slave and wage labour, and fight other bodies in the name of the colonizing state. (Sylvester 2006:68)

As Simon Cole (2002:63) has pointed out, for the British, fingerprinting was an invention of colonial bureaucracy, in response to the "problem of administering a vast empire with a small corps of civil servants outnumbered by hostile natives." Aboriginal peoples in particular were required to submit themselves to tests of "authenticity" (continued in a certain form today) to categorize ("full-blood" from "mixed-blood") and document for the purposes of expropriation and segregation (Pugliese 2010:44). In other words, the premise of colonial bureaucracy was controlling, documenting, and categorizing colonized populations biopolitically. These practices were — much like contemporary claims about biometrics — thought to be scientifically sound, rational, and free of personal bias. As a strategy of control over foreign populations, today's biopolitical regimes of knowledge are a means of colonizing the body, "overlaying it with calculatory grids and geometrically inscribing it with formulae that will transform it into an object of knowledge and power" (Pugliese 2010:45). Military biometrics, compared to those programs administered by governments to their own citizens or people wishing to enter, though not consensual in any meaningful sense, are also different from the subjection of occupied populations to regimes of surveillance that neither they nor their governments control. Military biometrics, as a tool of occupation in conflict zones, promise a new means of controlling both subject populations and global circulation.

Integrated into Western military strategy, biometric technology forms a key component of the rise of information technology in the global struggle for power and knowledge. It represents a quest for knowledge of "others" and its manipulation into usable military intelligence (Porter 2009). In this vein, early proponents articulated biometric technology as promising "identity dominance" in counterterrorism operations. Biometric technology is claimed to advance US control to the immaterial domains of risky borderland identities. As John Woodward, a key proponent of identity dominance asserts:

> Just as the U.S. military has established its superiority in other arts of war, now, working with other U.S. Government organizations, it must strive for identity dominance over terrorist and national security threats who pose harm to American lives and interests. (2005:30)

Seizing the biometrics of occupied populations who reside in fragile conflict environments is envisioned as a central aspect of waging war by other means.

The search for identity dominance can be understood as part of the globalization of control (Bonditti 2004). A key shift in international affairs since the end of the cold war has been the collapse of the dichotomy between the national and international realms in political thinking (Duffield 2007:185). This trend has only accelerated in the contemporary era of counterterrorism. The safety of national populations in the homeland is thought to be inextricably linked to securing populations in distant lands. The international society of the post-cold war era is embroiled in an resurgent level of interventionary permissiveness (Finnmore 2003; Wheeler 2000). The deepening consensus that the security of states is inextricably tied to the security of populations, in a somewhat contradictory fashion, has meant a greater willingness on the part of the UN, donor governments, and aid agencies to intervene in strife-ridden countries in a effort to quell violence, save lives, and orchestrate regime change. With increasing integration of military, humanitarian, and peace interventionism, a concerted regime of pacification has emerged in which formal sovereignty persists, yet "sovereignty within ineffective states is now internationalized, negotiable, and contingent" (Duffield 2007:185). Effective states are prepared to deploy technologies and tools to operate directly on the populations of ineffective states "to a degree unseen since the colonial period" (Duffield 2005:143). Unseen, here, should not be conflated with nonexistent. Rather, nationalist, anticolonial movements following the second world war were often inflected with the hegemonic desires of cold war superpowers, resulting in proxy wars and puppet regimes throughout the third world. What is perhaps remarkable, however, is the degree to which intervention and external regime control by Western coalitions are today regarded as largely benevolent and necessary (Ignatieff 2003) within an emerging liberal "consensus" in which intervention is supposedly forged on humanitarian grounds rather than apparent ideological ones. Indeed, this is an era of respectable liberal imperialism that upholds cosmopolitan values while containing circulation among the world of peoples (Duffield 2005:144).

Matters of intelligence, governance, and order within borders have consequently taken on a new level of importance in international security. With internal security now seen as an external concern and vice versa, sites of overlap between military and police have multiplied (Bigo 2001; Dubber and Valverde 2006). Unsecured circulation among networks of global population are now essentially equated with international danger, generating new markets for the securitization of identity. There is a concerted internationalization of an "identity industrial complex" (Browne 2010) that is indicative of these developments. Harvesting the biometric data of occupied and conflict-affected populations by foreign powers and organizations, is part of contemporary regimes that are out to police global circulation (BIMA 2012a:Video; Woodward 2005). Under this regime, the "good" circulation of licit commodity flows of goods and services, skilled migration and tourism is to be encouraged and supported, while the "bad" circulation of contraband, terrorists, and traffickers, and those not rich enough to consume, may be subject to interdiction. However, the policing of global flows is hardly as seamless as it is often portrayed. Biometric scanning of Afghan civilians, for example, has raised concerns that the wrong people are being flagged. There are Afghans all over the country who "claim that they were wrongly denied foreign visas or jobs after a biometric scan flagged up their presence on some watch list" (*Economist* 2012). The involuntary, secret nature of the programs, in which evidence is rarely divulged, has left people with little sense of how to challenge wrongful identification. Identification on a watch list, moreover, may be tantamount to conviction. On the one hand, policing global circulation aims to protect mass consumer society from non-state threats and on the other hand, it accounts for the fact that much of the global poor will be denied authorization to move and travel largely on the basis of their country of origin and the foreign policy objectives of the US and its allies. These wards of a global society are contained by fear and suspicion that they might destabilize "international society's finely balanced and globally interconnected way of life" (Duffield 2007:187). The globalization of control combines the physical management of flows of people attempting to penetrate territorial space and the assignment to people of their "rightful and precise place and identity" (Bonditti 2004:472).

One way to make sense of the global control of circulation and its connection to the growth of a global identity industrial complex is in relation to Foucault's (2003a) documentation of the rise of inclusive, productive, regimes of governance which he likened to intricate levels of surveillance cast over plagued cities of the medieval period. "All that was observed was recorded, permanently, by a visual examination and the re-transcription of all information in registers" (Bonditti 2004:476). This idea accounts for the tendency of this regime of power towards mass registration and the "ultratechnologization of surveillance" in a "globalized state of plague in which everybody is a potential plague victim" (2004:477). This process is reflected in the idea of identity dominance which calls for military biometric programs to be multitheatre, multiservice, multifunctional, and multibiometric (Woodward 2005:32). That is, military biometrics are designed to stretch across all theatres of operation, the entire military service, and be usable for various government departments from Homeland Security to the Department of State to the US military, and also include several different biometric modalities and record types (fingerprints, palm, face, iris, DNA, voice, and so forth). Additionally, it is reflected in BIMA's command structure which prioritizes the development of a "global application of biometric technology" and to achieve "seamless interagency interoperability" (BIMA 2013).

Today, a notable shift is discernible towards preemptive, risk-based, and preventative strategies that are eclipsing the national-international divide. More than ever before, threats are understood as migratory calling forth mechanisms that scan agencies, missions, and technologies. As the same time, these developments are discriminatory both in terms of the science of the technology and its application. In the case of exporting biometric technologies to interventionary zones, the discrimination has been globalized. As counterterrorism and counterinsurgency policies are motivated by anxieties that dangers from the South will wash up on the shores of the North, there is a Western regime of global surveillance demonstrated by the rolling out of military biometrics. In the double-headed coin of modernity (Gregory 2004), it is the populations of fragile states under occupation by foreign military and international organizations who are the objects of documentation. There is, consequently, a imperial dynamic to the politics of biometric visibility. Indeed, in the colonial present effective states have unmitigated, biopolitical access to the populations within ineffective ones. As an inclusive regime of surveillance, military biometrics are one aspect of the US-led global control of circulation.

Biometric Laboratories

In his analysis of fascism Walter Benjamin noted that "the harshest, most disastrous aspects of imperialist war are in part the result of the gaping discrepancy between the gigantic power of technology and the miniscule moral illumination it affords" ([1930] 1995:159). Contrary to not only fascist but also widespread belief, the outcome of war is not determined by valour. Rather, victory is decided by the discrepancy between wealth and poverty; the contradictions of capitalism. The export of biometric programs to crisis environments demonstrates the power inequalities that Benjamin highlights. The most obvious is that deploying expensive, high-tech machinery for use mainly on vulnerable people under siege, many of whom are living at or below subsistence levels, and are not in a position to refuse, is itself a moral chasm.

On the more procedural side of the issue, the use of biometrics by the US military and NATO does not appear to be accompanied by voluntary, informed consent or a clear policy on privacy protection. Adult men, residents of towns under investigation, and anybody wishing to repatriate or return home from internal displacement, access coalition affiliated employment or services, are required to submit to documentation. How or with whom their body data is shared is beyond their control and it is not clear that there is a process in place to govern how data is used. For example, BIMA's Annual Report, which oversees biometric operations for the US Department of Defense provided vague mention of privacy and storage (BIMA 2011:29–31). Despite being responsible for upwards of six million data sets (BIMA 2012b), the main focus was on homeland security and "protecting the war fighter." In terms of local control, the host Government of Afghanistan is now eagerly funded by the US to expand compulsory enrollment to every Afghan citizen, despite the fact that such measures would be illegal if administered to the populations of most European nations (Nordland 2011). Hence, the enrollment programs represent a probable lapse of rights and responsibilities among occupying powers, host governments, and subject populations, despite the claims of counterinsurgency strategy to be attentive to human rights and good governance (US Army and Marine Corps 2006).

One way to make sense of the ostensible coercion and lack of consent attached to military biometric technology is that it is in its infant stage of development. If so, then the peoples on whom it is practiced may be test subjects for wider regimes of surveillance. Such an idea is not farfetched as biometric technology has been used for some time by international agencies in crisis environments. For example, the UNHRC implemented a program requiring, upon repatriation, capturing the biometrics of Afghan aid recipients in an effort to curb "double-dipping" of aid packages (Jacobsen 2010). The program represents an instance of humanitarian experimentation on a highly vulnerable population. This population was made even more insecure as the enrollment design was perfected, suggesting that the program was at least partly about making biometric design safe and workable for "valuable subjects, often colonising, white and male subjects, who engage with technologies once they have been 'certified'" (2010:90). Meanwhile, Afghan refugees served as testing grounds to work out the "kinks" in the system.

Military biometrics reflect a similar spirit of experimentation. Indeed it was not until 2006 that biometric technology really emerged as an "in theatre" weapon. First there was the Biometrics Task Force (proposed as a temporary enterprise). It transitioned into the more enduring Biometric Identity Management Agency (BIMA) in 2010. Today BIMA has embraced its role as an adaptive and creative organization, declaring itself to be a future oriented enterprise in which the possibilities for knowledge control are limitless "including identity assurance, access control, and force protection, as well as new uses that are yet to be discovered" (BIMA 2012c). In line with this view, the agency reports that it has been focusing on hosting experimentation events that have "culminated in final preparations for in theatre pilots" (BIMA 2011:18).

One experimental venture is the development of "non-cooperative biometrics" (BIMA 2011:18; TR2 2010). In order to reliably capture iris patterns subjects must stand at close range (under two meters) for a minimum of three seconds. This requirement "restricts the range of domains where iris recognition can be applied, specially those where the subject's cooperation is not expectable" (Proença 2006:v). Noncooperative biometrics seem to be connected to recent investment in "second generation" systems, which tend to be more focused on profiling people on the basis of prediction, using movement or behavioural patterns of the body, gait, or "biological traits" (such as DNA, heat, smell, electrocardiogram) (Sutrop and Laas-Mikko 2012:21). Shared between these two is the focus on the development of advanced software tools capable of capturing people's biometrics (face recognition, iris scan, walking or movement form, speech) in public spaces *at a distance*. That is, this emergent technology is poised to capture peoples' biometrics without their consent or knowledge. Anticipating the strategic advantage offered by a covert system of surveillance, BIMA is funding a program at Carnegie-Mellon University, to develop "a vehicle-mounted camera system" that from up to 12 meters away, will automatically capture iris and facial scans (Evans 2012). As suggested, noncooperative biometrics may indeed offer a new form of "enemy surveillance" (Evans 2012). It also offers the chance to scan whole populations deemed problematic or risky. It is one way forward in the trend towards automating warfare. The course underway suggests that spaces of the global South deemed to be terrorist havens, actual or perhaps even potential zones of conflict are key targets for the development and implementation of new regimes of securitization.

This pattern of activity is consistent with experiments in preliberal government that animated colonial rule. As Nikolas Rose notes

> Whilst in the metropolitan polities liberal concerns halted the tendency for disciplinary technologies to be utilized directly in the name of 'reason of state', many of these technologies were deployed in colonial government. (1999:107)

Colonial modes of governance were also experiments in public order, involving the regulation of local soldiers through hierarchy and subordination, the construction of model villages, the use of colonial prisons as sites for elaborate experiments in medicine and physiology. These experiments rendered colonized peoples and spaces as laboratories for the limits and possibilities for disciplinary rule (1999:108–111). Though the hierarchy of relations between the North and South is not one of direct colonial control, in attempting to secure the identity of crisis populations — and by extension the future — there is a rejuvenation of earlier forms of colonial governance evident in the patterns of illiberal governance over subject populations in which local control is circumscribed by coalition mandates, sovereignty is contingent, and practices that are legally taboo in metropolitan settings are permissible in borderlands settings.

Conclusion

The growth and development of military biometrics may be one of the key vectors for the further development of biometric technology, not least because it can be deployed in places where people lack the rights and institutional power to challenge them. A mere five years ago Western militaries regarded biometrics as unconventional add-ons to existing operations. Today, however, they are considered to be integral "game changing" weapons in countering terrorism and insurgency in conflict environments. One important way of critically interrogating these developments is in terms of their racial politics.

This article has suggested that a global racism underpins military biometrics. In part this is connected to the racial assumptions that guide the technology. Rather than neutral authenticators of identity, biometrics contain built-in stereotypes about gender and race, as well as assumptions about the living spaces in which they are activated. On the global scene, military biometrics are emerging as key information technologies in the global struggle for power and knowledge that animates the war on terror. Biometrics promise identity dominance for the US and its allies over southern spaces and peoples rending them suspect identities. Demonstrating a return to earlier colonial modes of rule, military biometrics are partly an experimental enterprise in social control over populations in crisis and under occupation. At the same time, the remarkable ease of weaponizing civilian technologies of control demonstrates the salience of arguments that distinctions between military and civilian realms, as well as war and peace, are overplayed (Cowen 2008; Dudziak 2012).

Despite the indelible march forward, however, biometrics are not without their failures and shortcomings. Design weaknesses aside, there are many instances of failure "in theatre." The US program in Afghanistan has been noted for its unpredictable outcomes. For example, one *New York Times* reporter with a Norwegian background volunteered for a fingerprint and iris scan through the BAT System. Unexpectedly, the system found a "match" and declared: "Deny Access, Do Not Hire, Subject Poses a Threat." The picture and name was that of Haji Daro Shar Mohammed, an Afghan man who is on terrorist Watch List 4 (Nordland 2011). There are also the rising numbers of "green-on-blue" attacks in which Afghan soldiers have turned their weapons on coalition forces.[1] Though the tactic is unsurprising, the fact that numbers have been steadily increasing alongside investments in biometric enrollment and forensic testing, is noteworthy. The point here, however, is not simply that there are wrinkles to be ironed out in the technology, but rather that the assumption that people are biometrically identifiable, that identity is stable, is flawed. Systemic models of categorization always contain ideal

[1] In 2012 there were more than 50 NATO soldiers killed in green on blue attacks, in 2011 there were 21, and in 2010 there were 11 fatal attacks and 20. The combined total in 2007 and 2008 was 4 attacks and 4 deaths (CBC 2012; Fekrat 2012, *Guardian* 2012).

types that only exist in actuality some of the time. In addition, given that the stability of governments relies on popular legitimacy, it would seem that biometrics may be counterproductive if a significant portion of local populations are unwilling to accept the imposition of technological identities in the place of conventional ones (Homs 2008). Seizing biometrics of civilians and treating them all as suspect seems itself to be a transgression of the human rights that the US and its allies claim to be cultivating. Hence, the practice may increase alienation among the population and foment opposition. For all the talk of "transferring responsibility" to the governments of Iraq and Afghanistan, the proprietary rights of such data remain with the US and NATO (Brewster 2009).

Exporting biometrics thus exposes an important contradiction at the heart of modern counterinsurgency. The very measures taken to secure the future are helping to produce conditions for distrust and fear. In the case of military biometrics, the search for intimate knowledge is actually an expression of radical estrangement. The knowledge that biometrics seek is designed for dominance and strategic maneuver, reinforcing distance and hierarchy between North and South. It thus serves as a renewed global racialization of knowledge that animates our colonial present.

References

Aas, Katja Franko. 2006. "The body does not lie": Identity, risk and trust in technoculture. *Crime Media Culture* 2(2):143–158.

Ansorge, Josef Teboho. 2010. Spirits of war: A field manual. *International Political Sociology* 4(4):362–379.

Barkawi, Tarak and Mark Laffey. 2006. The post-colonial moment in security studies. *Review of International Studies* 32(2):329–352.

Bauman, Zygmunt. 1989. *Modernity and the Holocaust.* Ithaca, NY: Cornell University Press.

Bell, Colleen. 2011. Civilianising warfare: Ways of war and peace in modern counterinsurgency. *Journal in International Relations and Development* 14(3):309–332.

Benjamin, Walter. 1995 (1930). Theories of German fascism. Pp. 159–164 in Anton Kaes, Martin Jay, and Edward Dimendberg, eds., *The Weimar Republic Source Book*. Berkeley and Los Angeles: University of California Press.

Bigo, Didier. 2001. The möbius ribbon of internal and external security(ies). In Albert Mathius, David Jacobson and Yosef Lapid, eds., *Identities, Borders, Orders: Rethinking International Relations Theory*. Minneapolis: University of Minneapolis Press.

BIMA (Biometrics Identity Management Agency). 2011. Annual Report: Fiscal Year 2011. Department of Defense, United States of America.

——— 2012a. Video: Theatre/AFGHANISTAN. Department of Defense, United States of America.

——— 2012b. Timeline. Department of Defense, United States of America. Available at: http://www.biometrics.dod.mil/References/Biometrics_Timeline.aspx.

——— 2012c. Website: Collaboration. Department of Defense, United States of America. Available at: http://www.biometrics.dod.mil/collaboration.aspx.

——— 2013. Command Brief. Department of Defense, United States of America. Available at: http://www.biometrics.dod.mil/Files/Documents/About/BIMA_Command_Brief.pdf.

Bonditti, Philippe. 2004. From territorial space to networks: A Foucaldian approach to the implementation of biometry. *Alternatives* 29(4):465–482.

Brewster, Murray. 2009. Journalists required to submit to biometric scan in Afghanistan. *The Canadian Press* May 5: ProQuest.

Browne, Simone. 2010. Digital epidermalization: Race, identity and biometrics. *Critical Sociology* 36(1):131–150.

CBC. 2012. Afghan soldier gets death for killing four French troops. CBC News World July 17: Available at: http://www.cbc.ca/news/world/story/2012/07/17/afghan-soldier-sentenced.html.

Cole, Simon. 2002. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge, MA and London: Harvard University Press.

Cowen, Deborah. 2008. *Military Workfare: The Soldier and Social Citizenship in Canada*. Toronto: University of Toronto Press.

Der Derian, James. 2003. The question of IT in IR. *Millennium: Journal of International Studies* 32(3):441–446.

Dubber, Markus and Mariana Valverde, eds. 2006. *The New Police Science: The Police Power in Domestic and International Governance*. Stanford: Stanford University Press.

Dudziak, Mary. 2012. *War Time: An Idea, Its History, Its Consequences*. Oxford: Oxford University Press.

Duffield, Mark. 2005. Getting savages to fight barbarians: Development, security and the colonial present. *Conflict, Security and Development* 5(2):141–159.

——— 2007. *Development, Security and Unending War: Governing the World of Peoples*. Cambridge: Polity Press.

Economist. 2012. The eyes have it: Biometrics and the Afghan War. July 12. Available at: http://www.economist.com/node/21558263.

Evans, Gareth. 2012. Biometrics: Redefining the phrase don't shoot until you see the whites of their eyes. Army-technology.com January 11: Available at: http://www.army-technology.com/features/feature_biometrics-redefining-the-phrase-dont-shoot-until-you-see-the-whites-of-their-eyes/

Fanon, Frantz. 1967. *Black Skin, White Masks*. New York: Grove Press.

Fekrat, Nasim. 2012. The root cause of green on blue attacks. Open Democracy (December 17): Available at: http://www.opendemocracy.net/opensecurity/nasim-fekrat/root-cause-of-green-on-blue-attacks.

Finnmore, Martha. 2003. *The Purpose of Intervention; Changing Beliefs about the Use of Force*. Ithaca, NY: Cornell University Press.

Fontan, Victoria. 2006. Polarization between occupier and occupied in post-Saddam Iraq: Colonial humiliation and the formation of political violence. *Terrorism and Political Violence* 18(2):217–238.

Fordyce, Doni. 2007. US military orders handheld iris devices. *Biometric Technology Today*. October: 12.

Foucault, Michel. 2003a. *Abnormal: Lectures at the College de France 1974–1975*. New York: Picador.

——— 2003b. *Society Must Be Defended: Lectures at the College de France 1975–1976*. New York: Picador.

Galula, David. 2006 (1964). *Counterinsurgency Warfare: Theory and Practice*. Westport, CT: Praegar Security International.

Gates, Kelly. 2011. *Our Biometric Future: Facial Recognition and the Culture of Surveillance*. New York: New York University Press.

Gold, Steve. 2010. Military biometrics on the frontline. *Biometric Technology Today* November/December: 7-9.

Gregory, Derek. 2004. *The Colonial Present: Afghanistan, Palestine, Iraq*. Malden, MA: Blackwell.

Guardian. 2012. Afghan Solider killed four French troops after watching US 'desecration' video. *The Guardian* January 25: Available at: http://www.guardian.co.uk/world/2012/jan/25/afghan-soldier-french-marines-desecration.

Haraway, Donna J. 1991. *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York: Routledge.

Homs, Andrew R. 2008. The new legs race: Critical perspectives on biometrics in Iraq. *Military Review* (January-February):85–94.

Ignatieff, Michael. 2003. *Empire Lite: Nation Building in Bosnia, Kosovo and Bosni*. Toronto: Penguin Canada.

Jacobsen, Katja Lindskov. 2010. Making design safe for citizens: The hidden history of humanitarian experimentation. *Citizenship Studies* 14(1):89–103.

Kelly, John, Beatrice Jaurequi, Sean Mitchell, and Jeremy Walton, eds. 2010. *The Cultural Turn in the War on Terror: Counterinsurgency*. Chicago: University of Chicago Press.

Kingsbury, Alex. 2008. The U.S. Army ramps up biometrics to ID Baghdad residents. *U.S. News and World Report*, May 1.

L-1 Identity Solutions. 2007. Mobile iris recognition to be used in US military BAT system. ProSecurity Zone. 11 September: Available at: http://www.prosecurityzone.com/News/Biometrics/Iris_recognition/Mobile_iris_recognition_to_be_used_in_us_military_bat_system_35.asp#axzz20QBifffp.

Magnet, Shoshana. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC and London: Duke University Press.

Maguire, Mark. 2009. The birth of biometric security. *Anthropology Today* 25(2):9–14.

Muller, Benjamin. 2010. *Risk, Security, and the Biometric State: Governing Borders and Bodies*. New York: Routledge.

Nanavati, Samir, Michael Thieme, and Raj Nanavati. 2002. *Biometrics: Identity Verification in a Networked World*. New York: John Wiley and Sons.

Niva, Steve. 2008. Walling off Iraq: Israel's imprint on U.S. counterinsurgency doctrine. *Middle East Policy* 15(3):67–79.

Nordland, Rod. 2011. Afghanistan has big plans for biometric data. *New York Times*. 19 November: Available at: http://www.nytimes.com/2011/11/20/world/asia/in-afghanistan-big-plans-to-gather-biometric-data.html?_r=1&pagewanted=all.

Patel, Rajeev and Philip McMichael. 2004. Third worldism and the lineages of global fascism: The regrouping of the global south in the neoliberal era. *Third World Quarterly* 25(1):231–254.

Petraeus, David. 2006. Learning counterinsurgency: Observations from soldiering in Iraq. *Military Review* LXXXVI(1):2–12

Porter, Patrick. 2009. *Military Orientalism: Eastern War Through Western Eyes*. London: C Hurst & Co.

Prickett, Corporal Chris. 2005. Coming to your town soon? Tracking locals with the BAT of an eye. *Marine Corps News*, March 28.

Proença, Hugo Pedro Martins Carriço. 2006. Towards Non-cooperative Biometric Iris Recognition. PhD Thesis. Department of Computer Science, University of Beira Interior, Portugal.

Pugliese, Joseph. 2007. Biometrics, infrastructural whiteness, and the racialized zero degree of non-representation. *Boundary* 2 34.2:105–133.

——— 2010. *Biometrics: Bodies, Technologies, Biopolitics*. New York: Routledge.

Razack, Sherene H. 2008. *Casting Out: The Eviction of Muslims from Western Law and Politics*. Toronto: University of Toronto Press.

Reid, Paul. 2004. *Biometrics for Network Security*. Upper Saddle River, NJ: Prentice Hall.

Rose, Nikolas. 1999. *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press.

Schwartz-Dupre, Rae Lynn. 2007. Rhetorically representing public policy: National Geographic's 2002 Afghan girl and the Bush administration's biometric identification policies. *Feminist Studies* 7(4):433–453.

Sepp, Kalev I. 2004. Best practices in counterinsurgency. *Military Review* (September-October):8–12.

Shachtman, Noah. 2007a. Iraq diary: Fallujah's biometric gates. *Wired: Danger Room* (August 31): Available at: http://www.wired.com/dangerroom/2007/08/fallujah-pics/.

——— 2007b. Iraq's biometric database could become "hit list": Army. *Wired: Danger Room* (August 15): Available at: http://www.wired.com/dangerroom/2007/08/also-two-thirds/.

——— 2010. Army reveals Afghan biometric ID plan; Millions scanned, carded by May. *Wired: Danger Room* (September 24): Available at: http://www.wired.com/dangerroom/2010/09/afghan-biometric-dragnet-could-snag-millions/.

Sun Tzu. 1971. *The Art of War*. Oxford: Oxford University Press.

Sutrop, Margit and Katrin Laas-Mikko. 2012. From identity verification to behaviour prediction: Ethical implications of second generation biometrics. *Review of Policy Research* 29(1):21–36.

Sylvester, Christine. 2006. Bare life as a development/postcolonial problematic. *Geographical Journal* 172(1):66–77.

TR2: Terror Response Technology Report. 2010. Army issues RFIs for non-cooperative biometric development. *Terror Response Technology* 6.22(October 27):17.

United States Army and Marine Corps. 2006. *Counterinsurgency: Field Manual 3–24*. Washington, DC: United States Army and Marine Corps.

Wheeler, Nicholas. 2000. *Saving Strangers: Humanitarian Intervention in International Society.* Oxford: Oxford University Press.

Woodward, John. 2005. Using biometrics to achieve identity dominance in the global war on terrorism. *Military Review* (September-October):30–34.

Colleen Bell's work focuses on how freedom, conflict, and political change are shaped by the politics of security. Her recent book: *The Freedom of Security* (UBC Press) examines how freedom has been reformulated in Canada's war on terror. Currently, she is conducting a project on the re-emergence of counterinsurgency doctrine in Western interventions. The project explores the integration of civilian technologies within the schema of war. She is focusing on how civilian knowledge and expertise, derived from development, humanitarian response, and, most recently, field of medicine, are utilized in military power.
colleendbell@gmail.com