COMMENTARY

Datamigrants

Biometrics and the global security complex

James C. Ross

Immigration politics has historically involved talk about whom to include in the body politic, and how to keep the rest out. Modern states, whose sovereign rights assume a monopoly over the legitimate movement of people across borders, have long sought ways to 'normalize' the quality, number and integration of immigrants. This primary, state-centred understanding of immigration has changed little over the years, apart from the standards and means that have regulated immigrant selection and exclusion in Western countries. However, state responses to the security gaps exposed on 11 September 2001 capitalized on and reinforced the post-Cold War trend to securitize immigration. Immigration policy, particularly in the USA and EU, has come to reflect the revival of reductionist and exclusionary attitudes that have appropriated the immigrant body into an expanding global security complex.

The reassertion of territorial and symbolic authority over migration flows seemed counter-intuitive in the 1990s, in that liberal states were generally tightening their restrictions against human movement, while simultaneously relaxing barriers to the flows of goods, information, capital and labour. Today, the security context looks markedly different, and there is a remarkable technology that is changing how states control the movement of people. Some advocates have even called it a 'silver bullet solution' in the fight against global terrorism. I am referring to biometric surveillance technologies, known generally as biometrics: the public use of which Giorgio Agamben has called 'biopolitical tattooing'.[1]

State responses to 'new' security concerns are generating new political spaces through the confluence of the state with bodily space, where political borders intersect with human bodies. The core Westphalian belief in spatial separation that has traditionally situated subjects *inside* states is being conceptually challenged as states expand their use of information technology and biometric systems. State sovereignty, thought to be withering under the dual forces of fragmentation and globalization, has found a visceral vessel: the human body.

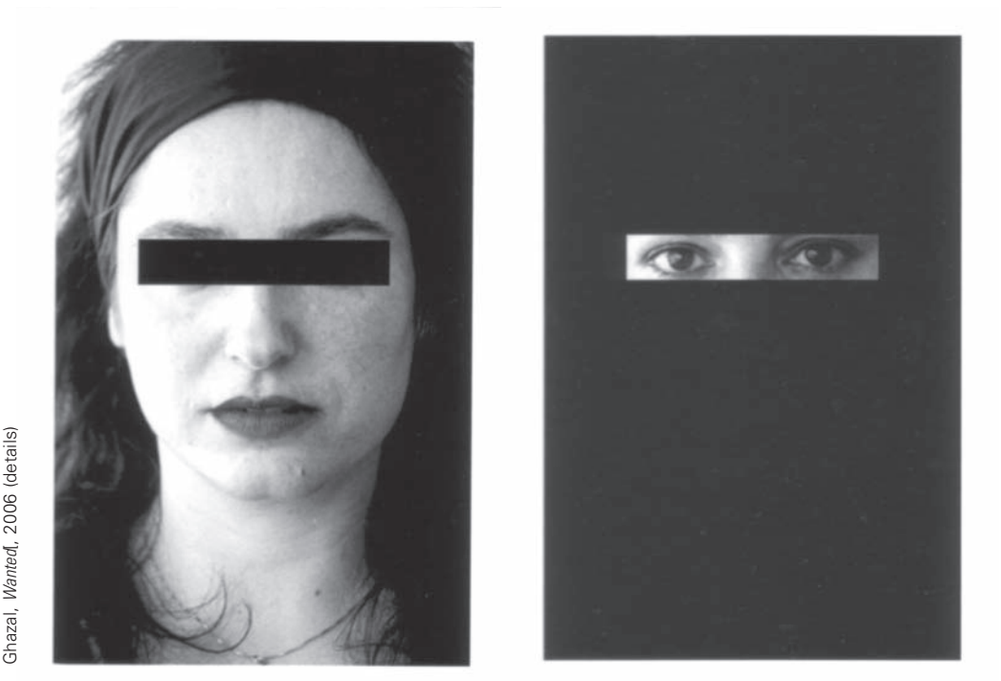
During the late nineteenth and early twentieth centuries, rapid urbanization, high levels of immigration, and growing ghettos of foreign-born populations ripened the conditions for a eugenic platform in the USA that appealed to state action towards the dual ends of racial preservation and population improvement. Just as the American Frontier had represented the line between the settled and the shifty, the pure and the profane, and the civilized and the savage of a maturing political body, immigrant bodies were likewise divided into fit and unfit, superior and inferior, desirable and undesirable. The immigrant body emerged on the scene as a new metaphorical territory to be controlled, conquered and incorporated, or excised and eliminated. Immigrants came to symbolize

the line between the national self and the foreign other, a physical marker, a fleshy reference that delineated domestic from alien bodies.

The old racial eugenics, based on organic and mechanistic body models, fostered a standard of assimilability that used mythical national origins to justify immigrant exclusion. Old ideas of immigrant control pursued the substantive transformation or total exclusion of immigrants based upon measures of their relative desirability and organic assimilability. The so-called 'melting pot' was a form of preprocessing – a homogenization of heterogeneous materials – towards the disciplinary ends of conformity and identity. In the United States, the immigrant body was the basis for the adoption of eugenic standards to determine immigrant desirability and promote 'racial fitness', eventually leading to the final closure of its 'Open Door' immigration policy with the passage of the National Origins Quota Act of 1924. Today, information and biometric technologies seek to individuate immigrant surveillance and significantly widen its scope, opening the way for new forms discriminatory categorization. Through this individuation, the old, visceral imagery of the body politic lingers in the discourses and technologies that are today defining the new bionetwork state.

The most notable metaphorical form of the political body, the *mechanistic body*, was inspired by the technological advances wrought by the Industrial Revolution. The advancement of Newtonian mechanics and a more prominent role for fluid mechanics (steam engines) and assembly-line industrial production in daily life affected how people interpreted and talked about their world. The efficient conversion of raw materials into finished products, what came to be known as mechanical rationalization, arguably prestructured assimilationist thinking and the development of the melting pot idea. By the early twentieth century, an evolving body/machine complex signalled a marked shift in the human–technology interface towards the machine ideal. More recently, out of revolutions in communications and information technology, the *bionetwork body* has emerged. Later metaphorical models do not replace earlier ones. Mechanistic and bionetwork bodies now make the organic political body a more complex, more multidimensional and, above all, more powerful body trope.

Yet something appears altogether different than before. The return of the actual body – albeit in digital form – as a site of state control puts into reverse the abstraction of the state into a metaphorical body of words and images. What we are witnessing in the



Ghazal, *Wanted*, 2006 (details)

new security context is the transubstantiation of the word, the body metaphor, back into the flesh.

Recent trends point to the continued growth of international migration. These flows may be legal or illegal, voluntary or forced. Since the end of the Cold War, the movement of people across international borders has evolved into a high security issue, and states are trying to meet this 'new' security demand with high-tech responses. Mass refugee movements, human trafficking, commercial sex, sophisticated drug cartels, and mobile terrorist cells – to name just a few – have combined to raise the importance of the migration–security nexus, prompting huge public investments in new technologies that link the state to the flesh of its subjects.

Most striking is how quickly the power to observe, monitor and track is being extended, normalized and legitimated in free societies, as new high-tech disciplinary practices move from the margins to the mainstream. The emergence of a bionetwork state incorporating disembodied datamigrants inaugurates a new stage in the evolution and intensification of cybernetic state control. Biometric surveillance represents what James Tully describes as the 'technological absorption of relations of power directly into relations of communications'. This is, he argues, 'the most revolutionary feature of the network age'.[2]

A perilous promise

What are biometrics, and what do they promise? The RAND division of Public Safety and Justice defines biometrics as 'any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual' (www.rand.org/publications/DB/DB396/). Biometric systems facilitate the digitization and electronic integration of people by reducing their biological and behavioural features to the lowest common denominator of the information age: bits of data. Rarely brought to public attention, however, are the new forms of classification, profiling and discriminatory categorization that biometric surveillance technologies make possible.

Biometric technologies enable the generation of new political spaces, new social classifications, and new forms of state control. One significant outcome of the marriage between biotechnology and information science is the extension of state control into virtual environments, electronic spaces where immigrants – and increasingly citizens – face new forms of disembodied integration and discriminatory categorization. Currently, biometric systems are chiefly used to identify, verify and classify the identity of a person on the basis of physiological or behavioural characteristics. Some examples of biometrics currently being tested and reviewed by public authorities and the private sector include: iris, retinal and fingerprint scanning devices, facial and voice recognition systems, dynamic signature verification, keystroke dynamics, among others. DNA identification, or the 'genetic fingerprint', is expected to become the quintessential personal identifier in the coming years, because of its easy measurability, robustness and high degree of distinctiveness. Advocates contend that DNA will provide an unambiguous way to link database records with individuals, making radically decentralized data integration possible and, as I argue below, new forms of human profiling and control inevitable.

Biometric systems do promise more reliable ways to identify and verify immigrant bodies to better track or restrict their access to entry, benefits and jobs. Industry advocates highlight lives being saved, lost children being found, and terrorists being stopped. One of the major claims in support of biometric surveillance is that these systems protect privacy by safeguarding one's identity. Identity theft, the argument goes, is a greater threat to individual privacy than the prospect of government or corporate mining of personal information.

The United States and the European Union have been testing, approving and implementing these new technologies for immigration control since the early 1990s. In the United States, the use of large-scale civilian biometric systems was being advocated well before the attacks of 11 September 2001. The Immigration Act of 1996 (PL 104–208) set up various pilot programmes authorizing the establishment and use of national databases and biometric systems to track criminal aliens, verify immigrant employment eligibility, and protect against document fraud. Emerging biometric surveillance systems raised widespread concern across the political spectrum. Orwellian fears about a national identification system and overzealous state intrusions into the lives of individuals were common rhetorical fodder. The attacks, however, would force even the most ardent critics of biometric surveillance to rethink their positions.

The USA–Patriot Act

Today's US policy on biometrics stems from Sec. 403(c) of the USA–Patriot Act (PL 107–56), signed into law just six weeks after the attacks, on 21 October 2001. It specifically directs the federal government to 'develop and certify a technology standard that can be used to verify the identity of persons' applying for or seeking entry into the United States on a US visa 'for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name'. The US Citizenship and Immigration Services, now under the auspices of the Department of Homeland Security, saw its budget for biometrics soar with the implementation of the US-VISIT Entry–Exit System, mandated by the USA-Patriot Act. US-VISIT uses biometric technology for the officially stated purpose to ensure that borders remain open to legitimate travellers but closed to terrorists. It is currently in place at 115 airports, 14 seaports, and 50 land border crossings across the country. Since US-VISIT came online in January 2004, more than 39 million visitors have been checked through the system, which currently requires non-resident foreign nationals to have their fingers and faces digitally registered upon entry to and exit of the United States.

These developments highlight a new dimension of border control, where the invisibility of 'virtual borders' embedded within data networks combine with the new visibility of biological features of human bodies, thus enabling novel forms of data integration, public surveillance and immigration control. Biometric technologies offer states new options for preventative tracking and restriction to keep 'illegal, criminal, and terrorist aliens' from entering national territories while ensuring the efficient (and traceable) flow of people, goods and services across international borders.

Most disturbing about biometric technologies is their built in 'data surveillance' or 'dataveillance' capabilities. Dataveillance refers to the collection of information about an identifiable individual from multiple public and commercial sources that may be assembled into character or behavioural profiles. Data profiling raises critical issues about the broader classificatory and discriminatory dimensions of biometric surveillance, not unlike those dystopian visions in popular films like *Gattaca* and *Minority Report*.

Furthermore, the widespread deployment of biometric surveillance systems is expected to increase the visibility of individual behaviour. Fears include the use of new forms of circumstantial evidence for criminal prosecution, increasing the possibility of wrongful conviction. Biometrics also makes it possible to match people's behaviour against predetermined patterns to generate suspicion or profile individuals, leading to new types of discriminatory categorization, blackmail and extortion. While some transgressions will undoubtedly be curbed, some prospective terrorists deterred, and some criminals apprehended, it is the law-abiding immigrants and citizens alike who will ultimately pay with their civil liberties and personal autonomy.

This is not only occurring in the United States. As the EU looks for common approaches to transnational issues like migration, crime and terrorism, a range of biometric options have emerged as an integral part of recent policy proposals. Current EU policy builds on the quiet electronic integration that has been taking place among Member States since the adoption of the Schengen Information System (SIS). The SIS system is the 'backbone' of the general agreement to open the EU's internal borders, whose scope is being significantly widened with the implementation of the SIS II, which increases the storage capacity and introduces new technological functions, most notably the broad inclusion of biometrics for the mandatory storage of digitized facial images and fingerprints of third-country nationals and, in the near future, all EU citizens.

Most of these developments and associated concerns about biometric surveillance have all but escaped notice by the citizens of Member States. With Britain rapidly expanding its global DNA database operated by Interpol, which has the largest percentage of its population recorded in a national DNA database (and urging other countries to do the same), troubling body politics loom ahead. Enter the high-tech yet silent cyber-side of the global security complex: no campaigns, no movements, no fittest family contests. The global security complex is a quiet merging of markets, states and military technology facilitated by powerful collection, storage, retrieval and profiling capabilities. Unlike earlier Orwellian models of surveillance, monitoring today is not about watching per se; what matters is recording.

The point of the global security complex, with its inter-operable connections between government and corporate databases, is to create the conditions for continuous latent surveillance, whereby the digital trails of individuals become accessible for on-call 'security' purposes. The global security complex emerges from the intersection of a rising global hegemon and its new global 'war' on terrorism; the increasing volume and diversity of global migration flows; and the global spread and interconnection of information and biometric surveillance technologies.

The global security complex has been further augmented by the disorienting speed and intensification of global financial and capital flows; the global marketing and distribution of goods, services and new forms of entertainment; the global trafficking of sex, drugs and children; the spread of global crime syndicates and global social and civilizational movements; and, without a doubt, the global military technology trade. None of these flows is discrete; all are increasingly interlinked by a vast informational network that belies traditional borders yet begets new controls. Rather than interrupt the speed of contemporary flows, liberal bionetwork states are adopting biometric technologies in an effort to monitor, filter and channel the intense circulation of back-and-forth human flows across their borders.

One of the aims of the global security complex is the connection, surveillance and disembodied integration of immigrant bodies and behaviours into global networks. Unlike earlier surveillance studies that characterized the nature of state control as centralized and panoptic, the surveillance environment today is a polycentric, nonhierarchical complex, where decentred and disembodied personal data flow unwittingly around the globe through vast and expanding informational architecture.

To sum up, in the polycentric and multidimensional environment of the new global security complex, the goals of states and private industry both collide and collude in a mutual bid to capitalize on new information and biometric technologies. In the emerging digital world, liberal internationalists of all stripes celebrate the goals of flexibility, mobility, openness and speed as information, services, images and people transcend and transgress old borders as never before. But states are (re)appropriating the same productive forces that have opened new political spaces for a generation of cyborg citizens, positioning themselves to make control imperative and escape

impossible. The uninhibited flow of personal data permits the (pre)constitution and preventive surveillance of virtual bodies when information is retrieved, reassembled and profiled for a multitude of purposes usually unbeknownst to the individual the data represent.

Arrival precedes departure

Security strategies currently being implemented include creating more layers of the border and facilitating the sharing of 'accurate' information within and among governments. These so-called 'high concept' approaches are included in the Smart Border approach currently being deployed in the USA and EU, an intelligence-based strategy that seeks to mainstream the virtualization of borders in ways that will have long-term implications for both immigrants and citizens alike. In this emerging field of state space, datamigrants merge with global data flows, forming part of a vast transnational network of surplus information. The migration of bodily and behavioural data both precedes and exceeds the real movement of real people. Moreover, new information technology makes it harder to perceive these practices of surveillance, especially when the presence may be predetermined. With disembodied integration, state control is no longer merely a means to an end, but the promised end in itself; 'control becomes the environment'.[3]

Datamigrants are only now beginning to flow across the Smart Borders of the emerging global architecture of communications networks. Classic migration involved departure, journey and arrival. The generalized exchange of instantaneous information and surveillance functions among bionetwork states has altered age-old assumptions about the journey. For datamigrants, this means arrival precedes departure.

Little by little, we are being disciplined to new forms of surveillance and – as immigrants, citizens and consumers – participating in the process through the 'voluntary' submission of bodily and behavioural information into innumerable private, public and law-enforcement databases, which are becoming increasingly interoperable. Overshadowed by the rhetorical vilification of immigrants and the symbolic reification of state borders has been the quiet appearance of biometric surveillance that will affect the life-chances of immigrants and citizens in liberal bionetwork states. The rhetorical conflation of immigrants with terrorists, smugglers and other criminals in the global security complex not only misrepresents immigrants who are more often the victims rather than the perpetrators of terrorism and crime, but it justifies measures of state control that are increasingly intrusive of privacy, invasive of bodies and discriminatory in practice. These developments have serious implications for how immigrants will be selected, integrated or excluded in the coming years.

In today's bionetwork world, we are all datamigrants, deceived cyborgs whose virtualized existence is tracked and profiled daily as our bodily and behavioural information flows back and forth across borders we never see. Compressed between the market and the state, we have been 'invited' to become participatory agents in a new global security complex whose totalizing promise belies the liberatory potential of the body–machine matrix envisioned by early cyborg enthusiasts. Lured by freedom and security, webs of state control are extending through our bodies and around the globe.

Notes

1. Giorgio Agamben, 'Bodies without Words: Against the Biopolitical Tattoo', www.germanlawjournal.com/article.php?id=371.
2. James Tully, 'Communication and Imperialism', www.ctheory.net/articles.aspx?id=508.
3. Paul Virilio, *The Art of the Motor*, trans. Julie Rose, University of Minnesota Press, Minneapolis, 1995, p. 131.