

# Biometric borders: Governing mobilities in the war on terror<sup>☆</sup>

Louise Amoore<sup>\*</sup>

*Department of Geography, University of Durham, South Road, Durham DH1 3LE, UK*

---

## Abstract

This article proposes the concept of the biometric border in order to signal a dual-faced phenomenon in the contemporary war on terror: the turn to scientific technologies and managerial expertise in the politics of border management; and the exercise of biopower such that the bodies of migrants and travellers themselves become sites of multiple encoded boundaries. Drawing on the US VISIT programme of border controls (United States Visitor and Immigrant Status Indicator Technology), the article proposes three central themes of the politics of the biometric border. First, the use of risk profiling as a means of governing mobility within the war on terror, segregating ‘legitimate’ mobilities such as leisure and business, from ‘illegitimate’ mobilities such as terrorism and illegal immigration. Second, the representation of biometrics and the body, such that identity is assumed to be anchored as a source of prediction and prevention. Finally, the techniques of authorization that allow the surveillance of mobility to be practiced by private security firms and homeland security citizens alike. Throughout the article, I argue that, though the biometric border is becoming an almost ubiquitous frontier in the war on terror, it also contains ambivalent, antagonistic and undecidable moments that make it contestable.

© 2006 Elsevier Ltd. All rights reserved.

*Keywords:* War on terror; Borders; Biometrics; Homeland security; US Visit; Risk

---

A technical matrix was established. By definition there ought to be a way of solving any technical problem. Once this matrix was established, the spread of bio-power was assured, for there was nothing else to appeal to: any other standards could be shown to be abnormal or to present merely technical problems. We are promised normalization

---

<sup>☆</sup> Earlier versions of this article were presented at the workshop of the British International Studies Association poststructural politics working group, University of Wales Aberystwyth, May 2005, and in the research seminar series, Department of Geography, University of Newcastle, June 2005.

<sup>\*</sup> Tel.: +44 0191 334 1969; fax: +44 0191 334 1801.

*E-mail address:* [louise.amoore@durham.ac.uk](mailto:louise.amoore@durham.ac.uk)

and happiness through science and law. When they fail, this only justifies the need for more of the same. (Dreyfus & Rabinow, 1983, p. 196).

Had information coordination technology been properly in place before September 11, the preattack activities of the hijackers could have been identified and prevented. There may have been a different outcome. (US House of Representatives, 2002)

### **Introduction: homeland security/borderland insecurity**

At a United States House subcommittee hearing in February 2002, a panel of commercial information technology experts and management consultants were asked to give technical advice on how the war on terror might be fought using risk profiling techniques. The hearing concluded that technologies designed to classify populations according to their degree of threat – long available in the private commercial sector – should be deployed at the service of border security. Indeed, the invited panel of experts stated clearly that ‘our enemies are hiding in open and available information’ and that, had surveillance and profiling techniques been in place, the events of 9/11 ‘could have been predicted and averted’ (*Accenture*, cited in *Kestelyn, 2002*, p. 8). In the immediate months following September 11, the dilemmas of the war on terror were being framed as problems of risk management, clearing the path for a burgeoning homeland security market that was to have implications far beyond the US ‘homeland’.

Two years on from the initial hearings, the US Department of Homeland Security (DHS) announced the *Smart Border Alliance*, headed up by management consultants *Accenture*, as the prime contractors for US VISIT,<sup>1</sup> a \$US10 billion project to restructure and manage all aspects of US air, land and sea port of entry security. The US VISIT programme, which I will use as my central point of discussion in this paper, represents one discrete example of a more prevalent phenomenon in the contemporary war on terror: the proliferation of risk management techniques as a means of governing mobilities.<sup>2</sup> *Accenture*’s self-styled ‘virtual border’, they promise, ‘is designed to operate far beyond US boundaries’, enabling the DHS to ‘assess the security risks of all US-bound travellers and prevent potential threats from reaching US borders’ (*Accenture digital forum, 2004*, p. 1). Under US VISIT, the management of the border cannot be understood simply as a matter of the geopolitical policing and disciplining of the movement of bodies across mapped space. Rather, it is more appropriately understood as a matter of biopolitics, as a mobile regulatory site through which people’s everyday lives can be made amenable to intervention and management.

In this paper I develop the concept of the biometric border in order to signal a dual-faced phenomenon in the contemporary war on terror: the turn to digital technologies, data integration and managerial expertise in the politics of border management; and the exercise of bio-power such that the body itself is inscribed with, and demarcates, a continual crossing of multiple encoded borders – social, legal, gendered, racialized and so on. The term biometric border, now part of the lingua franca of the risk consultants and the government departments charged with fighting the war on terror, has yet to be analysed critically in terms of how it is being deployed. As a manifestation of what *Walters (2002, p. 571)* calls the ‘biopolitical

<sup>1</sup> United States Visitor and Immigrant Status Indicator Technology.

<sup>2</sup> The research discussed here focuses specifically on the deployment of technologies for the governing of the mobility of people. However, the implications for the governing of the mobility of money/finance (see *Amoore & de Goede, 2005; De Goede, 2003*); and the mobility of goods are significant.

border', biometric borders extend the governing of mobility into domains that regulate multiple aspects of daily life. Subject to biopower, the crossing of a physical territorial border is only one border crossing in a limitless series of journeys that traverse and inscribe the boundaries of safe/dangerous, civil/uncivil, legitimate traveller/illegal migrant.

In part, then, the biometric border signals a new and important geographical imagining of the border, interpreted in the literature as symptomatic of both decentred and outsourced forms of state and the contradictions of contemporary global capital (see Hyndman, 1997; Newman, 2001). Yet, it is not simply the emergence of new border regimes but the performing of the *idea* of the biometric border that is becoming so central to the technologies of the war on terror. Rather as Dear and Lucero (2005, p. 317) suggest in their discussion of the Baja California borderlands, 'la frontera portátil is everywhere'. In effect, the biometric border is the portable border par excellence, carried by mobile bodies at the very same time as it is deployed to divide bodies at international boundaries, airports, railway stations, on subways or city streets, in the office or the neighbourhood. The work of the biometric border is thus the work of redefining what Bigo (2001, p. 112) calls the 'Möbius ribbon' of internal and external security, such that 'internal and external security become embedded in the figure of the "enemy within", of the outsider inside, increasingly labeled with the catchphrase "immigrant"'. Read through Bigo's (2001, p. 100) lens of a governmentality that combines 'technological sophistication with the old disciplines of the body', immigration and the terrorist threat become combined as a problem 'not because there is a threat to the survival of society' but because 'scenes from everyday life are politicized, because day-to-day living is securitized'. Thus, the governing of mobility through US VISIT's biometric borders is categorically not about new border threats in a post-9/11 world, but rather a means of identifying and designating the safe from the dangerous at multiple borders of daily life. US VISIT, then, is but one element of a liberal mode of governmentality that sees risk profiling in the war on terror pervade and claim every aspect of species life itself, or something akin to a shift from geopolitics to biopolitics (Dillon, 2002, 2004; Dillon & Reid, 2001; Larner & Walters, 2004).

Certainly such biopolitical and governmental techniques and technologies capture a crucial aspect of what is at stake politically in the extension of the biometric border into multiple realms of social life, and this will form a key part of my argument. Yet, here I am also seeking to sound a note of caution lest, when we advance a critique of biopolitical systems in the war on terror, we inadvertently reproduce the certainties and assurances of the technical matrix that has become the mainstay of the homeland security programmes. The authority of risk profiling in the war on terror precisely relies upon the representation of a world that would be safer if only ambiguity, ambivalence and uncertainty could be controlled. In effect, the place of science and technology in fighting the war on terror is ever more secured if we overstate the coherence of the grip it has on life itself. As Dillon (2004, p. 82) reminds us, 'species life is not a datum, it is an undecidable'. Though the biometric border undeniably draws species life into the exercise of power, it is necessarily working with an unstable and unpredictable referent. Throughout this paper I will suggest ways in which the ambivalent, antagonistic and undecidable moments of the biometric border might be revealed. Though, as Foucault (1976, p. 93) conceived it, there may be no 'single locus of great Refusal' or overt resistance to the use of risk profiling as a means of governing the movement of people, there are moments of dissent and multiple instances of tension that reveal the contingent and incomplete nature of the programmes.

The discussion that follows will explicitly hold together two arguments that are apparently in tension: that the biometric border may be becoming a ubiquitous deployment of risk profiling in

the war on terror; but that this ubiquity is always also necessarily disrupted and disruptive. The argument draws on the US VISIT programme to discuss in turn three central themes of the politics of the biometric border. First, I look at the use of risk as a means of governing in the war on terror, based on dividing practices that segregate ‘legitimate’ mobilities (business, travel, leisure and so on) from ‘illegitimate’ mobilities (terrorist, trafficker, immigrant and so on). Second, I discuss the representation of biometrics and the body. Biometric data are assumed to be anchored in the human body, apparently fixing and securing identity as a basis for prediction and prevention. Finally, I draw out the processes of authorization that are allowing the surveillance of mobility, and particularly of migrant mobilities and legalities, to be practiced in everyday life, from private security firms to technology-enabled people on the city street or subway network.

### **Risk and mobilities in the war on terror**

Announcing his plans for the US VISIT programme to European political leaders, former US Secretary of Homeland Security, Tom Ridge, depicted a globalizing society of simultaneous opportunities and threats. ‘As the world community has become more connected through the globalization of technology, transportation, commerce and communication’, he argued, ‘the benefits of globalization available to peace loving, freedom loving people are available to the terrorists as well’ (Department of Homeland Security, 2005, p. 1). Framed in this way, the problem becomes one of isolating the legitimate ‘inside’ transborder activities of the global economy, and securing them from the illegitimate ‘outside’ of those who would exploit the possibilities of open borders. I have argued elsewhere, following Pat O’Malley and others, that the discursive deployment of risk, particularly by management consultants, is closely allied to the representation of the risks and rewards of globalization (Amoore, 2004; De Goede, 2004; O’Malley, 2000). Far from seeking to minimize or limit the risks of a globalizing society, the new techniques of ‘targeted governance’ in the war on terror rest upon an ‘embracing of risk’ made possible by the global integration of information technologies (Baker, 2002; Valverde & Mopas, 2004, p. 239).

It is precisely such a vision of embracing the risks of globalization via information technology that frames the Department of Homeland Security’s US VISIT programme. Put simply, US VISIT appears to hold out the possibility of reconciling the necessary fiction of porous international borders that are open for business, with the need for security at the border. It does this by enacting a series of dividing practices in which the subject is broken up into calculable risk factors, both within herself (such as, for example, ‘student’ and ‘muslim’ and ‘woman’), and necessarily also in relation to others (as, for example, ‘alien’, ‘immigrant’ or ‘illegal’). It is through such dividing practices that, for Foucault (1983, p. 208), the subject becomes objectivised. Though it is beyond the scope of this paper to discuss the implications of what has been called ‘dataveillance’ in the war on terror (see Amoore & de Goede, 2005), suffice to say that these techniques involve processes of objectivisation in which new technologies of surveillance identify ‘what effectively become suspect populations or “risky groups”’ (Levi & Wall, 2004, p. 200; see also Clarke, 1994).

*Accenture’s* ‘smart border solution’ to the governing of mobilities rests upon just such a system of dataveillance that categorises populations into degrees of riskiness. It does this by interfacing and integrating, at the time of writing, over 20 existing databases, from police authorities, to health, financial and travel records. Among the most significant are IDENT, a biometric database that stores and identifies electronic fingerprints on all foreign visitors, immigrants and asylum seekers; ADIS, storing travellers entry and exit data; APIS, containing

passenger manifest information; SEVIS, containing data on all foreign and exchange students in the United States; IBIS, a ‘lookout’ watch list interfaced with Interpol and national crime data; CLAIMS3, holding information on foreign nationals claiming benefits; and an array of links to finance and banking, education, and health databases. US VISIT uses these databases to profile and encode people according to degrees of riskiness, checking ‘hits’ against passenger manifests and visa applications. As one *Accenture* consultant put it: ‘...the old systems could really only check the single person who is walking out to the plane. *Accenture*’s system will check your associates. It will ask if you have made international phone calls to Afghanistan, taken flying lessons, or purchased 1000 pounds of fertilizer’ (cited in “[The Price of Protecting the Airways](#)”, 2001, p. 1). The guiding assumption, then, is that encoded risk profiles can be used as a basis to predict and prevent future acts. What Van Munster (2004, p. 142) has called a ‘discourse on eventualities’ has allowed the war on terror to be fought preemptively through risk profiling. The risk-based identity of the person who attempts to cross an international border is in this way encoded and fixed far in advance of reaching the physical border – when, for example, he leaves the electronic traces of buying an air ticket, applying for a visa, using a credit card, and so on. Indeed, the *Smart Borders* authorities hail US VISIT precisely because ‘it makes US border guards the last line of defense, not the first, in identifying potential threats’ (*Accenture digital forum*, 2004, p. 4).

It is this preemptive fixing of identities that is emerging as a key point of contradiction and tension within the logic of the biometric border, and is of central concern to advocacy groups, civil liberties and privacy organizations, and immigrant rights groups. In April 2004, a coalition, including the Arab-American Anti-Discrimination Committee, National Immigration Law Center, Electronic Privacy Information Center (EPIC), and American Civil Liberties Union (ACLU), wrote to the DHS expressing their concern at the ‘enormous potential for error and violation of international human rights standards’ in the US VISIT system.<sup>3</sup> Of particular concern to the group is the question of what happens to people who come up as ‘hits’ on the various databases, and how a ‘false hit’ that leads to detention or deportation can be challenged.<sup>4</sup> As one EPIC lawyer put the problem: ‘these technologies are assumed to provide a complete picture of who someone is, leaving people having to dispute their own identity’.<sup>5</sup> In these terms the US VISIT system far exceeds a technologized ‘recording’ of entry and exit of non-US citizens and ‘matching of people to their travel documents and visas’ (*Accenture digital forum*, 2004, p. 2). Rather, by encoding people with a pre-determined risk profile, US VISIT engages in what has been called ‘the legitimation work of globalization’, the everyday work of ‘issuing and denying documents, sealing and opening records, regulating and criminalizing transactions, and repudiating and claiming countries and persons’ (Coutin, Maurer, & Yngvesson, 2002, p. 804). The mastery of border risks by governments and their business partners, then, is undertaken on the back of risk displacement – the reallocation and intensification of uncertainty for the most vulnerable groups.

The direct and organized efforts to resist the governing of mobility in the war on terror, exhibited by the ACLU, EPIC and others, are playing an undeniably important role in politicising a programme that has been so effectively depoliticised. Yet, in many ways the appeal to privacy

<sup>3</sup> Full text of the letter is available at [www.epic.org/privacy/usvisit/redress\\_letter.pdf](http://www.epic.org/privacy/usvisit/redress_letter.pdf).

<sup>4</sup> Haitian-American novelist Edwidge Dandicat’s uncle, the Reverend Joseph Dandicat, died of Pancreatitis in Department of Homeland security custody in 2004. The relatively high profile of rev. Dandicat’s death provoked widespread questioning of US VISIT procedures by groups representing immigrant communities.

<sup>5</sup> Interviews conducted at EPIC, Washington DC, November 9, 2004.

laws and civil liberties suggests that US VISIT has somehow failed administratively, or failed to correctly include particular groups, so that if only the recount could include specific groups with legitimate claim to cross the US border, the problem would be fixed. Meanwhile, the sense that a line can be drawn between those with legitimate claims to mobility and those whose claims are somehow dangerous is not at all destabilised by the interventions of privacy and civil liberties groups. While their interventions are crucial in challenging specific instances of abuse and suffering, it is perhaps in other spheres that we find instances of the politicisation of the techniques used at the biometric border.

In common with others who have pointed to the capacity of the satirical and playful practices of the arts to disrupt our sense of the ‘normal run of things’ (Bleiker, 2000; Butler, 2004; De Goede, 2005), I am going to suggest here that artistic interventions in the governing of mobility point to important, and often neglected, forms of dissent. The very month that the US VISIT contracts were announced, British artist Heath Bunting missed the opening of his show, *Status Project*, because he was refused entry to the US. Bunting’s work, commissioned by the *Tate Modern* and the *New Museum of Contemporary Art*, explores the playing out of the politics of the border in the domains of status and identity. The viewer is invited to use a series of databases to secure a new identity (and ultimately a false passport) through the use of ‘junk IDs’ such as DVD membership cards (“*Rules of Crime*”, 2004). Described by the *New York Times* (“*How to Cross Borders*”, 2004) as ‘the Department of Homeland Security’s worst nightmare: a road map enabling all kinds of undesirables to penetrate a nation’s borders, banking systems and supermarket loyalty clubs’, Bunting’s project mimics and parodies the representations made by systems such as US VISIT. The artist describes his work as ‘looking for loopholes in the social grid’, acknowledging that ‘this is knowledge that could be used as a weapon’, but suggesting that ‘it’s the same as giving someone a street map. It could be used to help prepare burglaries or riots, but it could just help you walk around’ (*New York Times*). Visually mapping the logics of integrated databases in a form reminiscent of the London Underground map, Bunting exposes the relationship between legal, political and social statuses: ‘if you are a blood donor’, states one of his data maps, ‘then you are not HIV positive, an injector of drugs, taking antibiotics, a prostitute, gay, or less than one year from having a piercing’. *Status Project* thus not only reveals the flawed and insecure assumptions on which systems such as US VISIT are based, but calls into question the apparent ubiquity and everyday prevalence of data-driven identifications and makes it possible to ‘talk back’ in a way that mimics the very discourse that it seeks to unsettle (Butler, 1997, p. 14).

## **Biometrics and bodies**

The deployment of electronic personal data in order to classify and govern the movement of people across borders has become a key feature of the contemporary war on terror. The US VISIT programme, though, extends the use of integrated personal data into biometrics, a move that signals what Levi and Wall (2004, p. 194) have termed a ‘new politics of surveillance’. To clarify this point, this is not to say that biometric identifiers have not historically been central to the governing of mobility – after all, signatures are a form of biometric (see Salter, 2003), nor that ‘older’ forms of surveillance are not still prevalent in the war on terror. Indeed, the historical emergence of body counts to enumerate and account for colonial subjects, as Appadurai (1996, p. 133) suggests in his discussion of systems of classification in colonial India, disciplines the ‘unruly body’, bringing it back into a zone of calculation and manageability, recuperating it and accounting for it within ‘normal’ ranges of acceptability. Contemporary

biometric body counts bare out much of what Appadurai signals for the creation of ‘boundaries around homogeneous bodies’ that ‘performatively limits their extent’, flattening differences and idiosyncrasies into calculable categories. New forms of biometric technology extend this categorization and enumeration of the body via processes of risk profiling, such that they have themselves come to perform and represent a border that approves or denies access.

The US Patriot Act defined a set of practices for biometric applications that afforded their almost unlimited use in the investigation and identification of terrorism. In effect, the US VISIT system converges the data from integrated databases with biometric identifiers such as electronic fingerprints, facial and gait recognition, and iris scans. Though the implementation of biometric gateways has been beset by difficulties, the seductive allure of biometrics has taken a strong hold in the governmentality of mobility.<sup>6</sup> Mike Davis, director of criminal justice for the FBI, for example, assured a conference of European technology companies that ‘the war on terror has come to rely on biometric technology’ in a world where ‘the only way to trace a terrorist is through biometrics’ (cited in “*Biometrics: Great*”, 2004, p. 17). The allure of biometrics derives from the human body being seen as an indisputable anchor to which data can be safely secured. What van der Ploeg (2003, p. 58) has observed as a gradually extending intertwinement of individual physical characteristics with information systems’ has served to deepen faith in data as a means of risk management and the body as a source of absolute identification.

Biometric technologies are perhaps best understood as techniques that govern both the mobility and enclosure of bodies, or what David Lyon has termed surveillance as ‘social sorting’ (Lyon, 2003a, 2003b; see also Cunningham & Heyman, 2004). In January 2005, for example, the then Secretary of the Department of Homeland Security, Tom Ridge, completed a number of agreements with the Dutch government to deploy biometric systems to accelerate the movement of ‘trusted travellers’ whilst restricting the movement of higher risk groups. Opening the new registered traveller programmes at Schipol airport, Secretary Ridge emphasized the possibilities for the categorization of air passengers via biometrics: ‘we can design border security initiatives to both enhance homeland security and facilitate global commerce and travel’.<sup>7</sup> Within these programmes, we see not only the intertwinement of physical identifiers with information systems, but the annexing of patterns of behaviour, and their associated identities, that can be afforded smooth movement across borders. The use of air miles databases, for example, is coupled to the biometric submission of an iris scan to produce the identity of a ‘trusted traveller’. Of course, Secretary Ridge himself qualifies for the programme:

A fingerprint or iris scan is all that is needed for quick passenger identification and expedited processing through security. I’ve enrolled in the program myself, and I can tell you that it is a great tool that helps move low risk travellers more efficiently so that resources can be focused elsewhere, where the need is greater.

(Department of Homeland Security, 2005, p. 1).

In a sense, the US Air Transportation Association’s registered traveller projects, together with the Netherlands’ Privium Plus, have much in common with the historical practices of

<sup>6</sup> Problems with the implementation of biometric identifiers led, for example, to the DHS delaying their initial requirement of biometric passports by October 2004. A litany of difficulties, including the clustering of facial recognition ‘false hits’ on black and Asian faces, led the DHS to admit that they had ‘bought a lot of stuff off the shelf that wasn’t effective’ (*New York Times*, May 8, 2005).

<sup>7</sup> Full text of speech is available at: [www.useu.be/terrorism/EUResponse/Jan1305RidgeNetherlandsProgram.html](http://www.useu.be/terrorism/EUResponse/Jan1305RidgeNetherlandsProgram.html).

what is called ‘risk pooling’ in studies of the insurance industry (cf. Ewald, 1991; Heimer, 2002). By categorizing patterns of behaviour as ‘low risk’ (whether in the profiling of claims history in insurance, or via frequent flier history in airline security), authorities group together for common treatment individuals who are classified and encoded with a similar category of risk – in this case expedited passage through security checks. Indeed, the trusted traveller is called into being through an array of self-governing techniques. The US VISIT in-flight video has an animated Tom Ridge warning that the traveller has the responsibility to record their own electronic fingerprint at exit kiosks in the departure lounges. Rather as a credit rating is derived from past patterns of responsible financial borrowing, the trusted traveller is the individual who governs his own mobility and establishes a low risk mobility rating.

In populations targeted for higher risk pools, of course, the electronic enmeshment of data with bodies is more invasive, and the degree of surveillance intensified. Whereas the *trusted traveller biometrics* tend to emphasize membership of (or inclusion in) a group based on pre-screening checks such as citizenship and past travel patterns, what I will call *immigrant biometrics* are based on ongoing surveillance and checks on patterns of behaviour. While for the trusted traveller the biometric submission is usually the end of the matter, the passport to ‘borders lite’ (if not to a borderless world), the risky traveller’s biometric submission is only the beginning of a world of perennial dataveillance where the border looms large. Regular travellers across the US–Mexico and US–Canada border, for example, can submit biometric data in order to fast-track the security checkpoint. Unlike Mr. Ridge’s frequent flier experience, though, on trial at the US–Mexico border are radio frequency identification (RFID) enabled smart cards, enabling the tracking of the holder’s whereabouts within the US.

In terms of what is at stake politically, the emerging contests around biometric borders centre on the question of the verification of identity. Biometric technologies are represented as infallible and unchallengeable verifiers of the truth about a person – the ultimate guarantors of identity. As such, they are increasingly being seen as the smart scientific solution to the problem of fighting the war on terror without impeding globalization – the means of managing risk by embracing risk (Baker & Simon, 2002) or, in Dillon and Reid’s (2001) terms, of fighting liberal war whilst securing the liberal peace. *Accenture*, for example, views the biometric aspects of US VISIT as ‘a key win in a climate where other countries on the front line of terrorism are interested in similar programmes’ (*Accenture press release, 2004*, p. 1). In the UK, US VISIT-compliant biometric passports, for example, have become the Trojan horse for the much-contested ID card, with all passport applications post-2008 compulsorily linked to an ID card (Lyon, 2004). The 2005 US ‘REAL ID’ Act is perhaps the strongest example of the move to positioning identification and credibility determination, particularly of immigrants and asylum seekers, at the heart of the war on terror. The Act will compel authorities such as drivers’ license bodies to verify identity and immigration status in the applications process. The linking of biometrics to integrated databases, as in all of these cases, not only appears to make the identification of a person beyond question, but also apparently lends authenticity and credibility to all of the data that are connected to that identity. Treated as a scientific, neutral and ‘smart’ solution to the problem of establishing identity (Valverde & Mopas, 2004), biometrics are parceled up, contracted out, networked and made available to multiple agencies with an anti-terror remit.

Yet, far from constituting a secure anchor for individual identity within the human body, biometric technologies are part of a process in which they ‘are themselves incorporated into the

bodily experience' (van der Ploeg, 2003; see also Thrift, 2004). It is important, then, to challenge and destabilise the apparent security of the biometrics-body-identity nexus, and to politicize the site of identity as a target for the war on terror. As Butler, Laclau, and Zizek (2000, p. 17) remind us, "'identity" itself is never fully constituted; identification is not reducible to identity'. Read in these terms, a project that works on fixing or securing an identity can never be complete, will always be contingent and uncertain. The ever-present gap between identity and identification, or what is unrealizable in the discursive making of the subject, has been a preoccupation of social and cultural theory for some time. Despite radical differences of approach, there is some sense of valuing the 'gap' politically as a potential space for contestation and dissent. Since the identity of the subject can never be entirely secured, the practices that rely upon the calling into being of specific subjectivities — terrorist, immigrant, asylum seeker — can never consider their work complete. For Bhabha (1994, p. 269), what is 'politically crucial' is the necessity of thinking beyond 'initiatory subjects and focusing on those *interstitial* movements or processes that are produced in the articulation of difference'. For Bhabha (p. 270) the interstices that emerge at the frontiers or borderlands of our contemporary world have particular significance — the struggles of the 'unhomed inhabitants' of migrant workers and refugees 'against the authorities' who seek to refuse them access.

Biometric technologies that identify and sort mobile bodies can be understood as one such frontier, where the unhomed inhabitants are produced through the marking out of sameness and difference. Something of the acute ambivalence of our subject positions at the biometric border is captured by artist Heath Bunting's 2002 work, *BorderXing*. A web-based work commissioned by Tate Britain and the Musée d'Art Moderne, *BorderXing* documents the artist's journeys across 20 international borders without identification documents. The work can be read partially as a 'how to' guide to crossing international borders without papers, delineating tactics and routes and offering advice: 'don't run if you are seen as you will probably be shot'; 'caution, ice could crack'. It contrasts the physical bodily demands of illegal border crossers (water, knowledge of the outdoors, survival skills, for example) with the body as guarantor of access via fingerprints or iris scans ("Rules of Crime", 2004). Ultimately, though, it is the artist's governing of access to the *BorderXing* site that reminds the viewer of the importance of establishing credibility and identity as the key to border crossings. The website is accessible from most countries of the global south, but to enter from the UK, US, Europe, Australia or New Zealand the visitor must apply to the artist and establish their credentials. In a world where frequent fliers become accustomed to access and open borders, Bunting fleetingly confronts the viewer with something of 'the everyday experience of illegal border crossers'. 'Today's borders are not so much about permission and refusal of entry as about user profiling', reflects Bunting, 'the ultimate aim being the filtering of presumably useful from non-useful border crossers' (interviewed by Schneider, 2002). The interstitial spaces envisaged by Homi Bhabha appear within Bunting's images as a continual provocation to the contemporary biometric border. His landscapes disrupt the sense of a border as a single line marked in territory and suggest instead a border that is inscribed in and through multiple political practices.

### Authority and authorization

In their discussion of the governmentalization of contemporary societies, Rose and Valverde (1998, p. 550) suggest that the 'authority of authority' has been established and defended 'through alliances between the different legitimacies conferred by law and expertise'. Understood though this frame, the rise of the biometric border represents just such a mode of

authority: conferred by a raft of anti-terror legislation stitched together with the expertise of the risk managers. The alliance between law and expertise noted by Rose and Valverde is part of what Foucault termed a ‘normalizing society’, in which the calculated administration of life is the key technology of power (Foucault, 1976, p. 144). The increasing hybridization of legal and non-legal authorities, as Rose and Valverde (p. 542) argue, draws on a continuum of regulatory apparatuses, from the strictly juridical to the professional and personal.

On announcing *Accenture’s* contract, for example, the Department of Homeland Security said that ‘by harnessing the power of the best minds in the private sector it is possible to enhance the security of our country while increasing efficiency at our borders’ (Department of Homeland Security, 2004). Similarly, *Accenture’s* Eric Stange talks of the *Smart Border Alliance* as ‘a strong team of highly qualified companies with significant border management expertise’ (*Accenture press release*, 2004, p. 2). For one of *Accenture’s* sub-contractors, *Titan Corporation*, some of this expertise was honed in the Abu Ghraib prison in Iraq, where they supplied interrogators and interpreters. Yet, very little of this has registered in public debate, beyond vague concerns about an offshore company winning a US government contract.<sup>8</sup> In effect, the expertise becomes the norm, as one immigration lawyer explained, ‘since 9/11 the public authorities have turned to the private authorities to design the architecture of the systems, to make “efficient systems”... so this is only ever treated as a technical problem, and not a question of politics’.<sup>9</sup>

The active depoliticisation that is enabled via the authorization of groups such as *Smart Borders*, however, does not imply simply a shift from public to private authority. Rather, the authority of the state is enhanced and revitalized, the apparent loss of sovereignty being ‘compensated through the resurgence of sovereignty within the field of governmentality’ (Butler, 2004, p. 56). Understood as examples of Butler’s resurgent ‘petty sovereigns’, the US VISIT disperses power throughout a network of authorities whose actions are sanctioned by a state that declares ‘exceptions’ to or ‘suspensions’ of the rule of law (Agamben, 2005; Butler, 2004). Connolly (2005, p. 145) makes an important point, then, when he argues, partially contra-Agamben, that ‘the sovereign is not simply *he* (or *she*) who first decides that there is an exception and then decides how to resolve it’. Instead, ‘sovereign is *that* which decides an exception exists and how to decide it, with the that composed of a plurality of forces circulating through and under the positional sovereignty of the official arbitrating body’. I am arguing here not that sovereignty is somehow lost by the state to private players, nor that authority has become governmentalized around the consultants and data integration multinationals. The authority to designate the exception and to produce the figures of the trusted traveller and Agamben’s (1998) abandoned figure of *Homo Sacer*, though, is diffused to the point that it is in the hands of all citizens. As Gregory (2004, p. 16) has captured the ‘banality of the colonial present and our complicity in its horrors’, so the proliferation of contemporary spaces of exception should not prevent us from attending to the mundane violences of ‘practices that mark other people as irredeemably “Other”’.

One effect of this dispersal of spaces of exception into the routines of everyday life has been what Coutin (2000) has called ‘the surveillance of migrant illegality’. In *Accenture’s* bid for the US VISIT contract, for example, they reportedly ‘wowed government officials with a demo that included wireless tags that tracked immigrants’ whereabouts’ (*“Accenture Hits the Daily*

<sup>8</sup> Interviewed in the *New York Times*, Representative Richard Neal declared the US VISIT contract to be ‘outrageous’. ‘The Bush administration’, he argued, ‘has awarded the largest homeland security contract in history to a company that has given up its US citizenship and moved to Bermuda’. ‘If companies want a slice of the American pie’, he declared, ‘then they had better help bake it’ (2004, p. 26).

<sup>9</sup> Interview, Immigration Law Center, November 7, 2004.

Double”, 2004, p. 74). Despite a legal framework that ostensibly restricts the deployment of US VISIT powers to border management, the potential to disperse US VISIT authority into the governing and surveillance of migrant workers was clear even before the award of the contract. The extra-legal authority conferred by expertise has enabled the bundling together of ‘terrorist’ with ‘illegal immigrant’, ‘welfare tourist’ and so on, authorizing an ever widening sphere of actors to engage in surveillance and policing.

In many ways, the emphasis on risk profiling embodied within US VISIT is merely an initial step in rendering ordinary and everyday the monitoring of suspicious or risky groups. Following the award of US VISIT, *Accenture’s* Eric Stange explained in an interview that what is ultimately required in the war on terror is a ‘cultural change’, a shift that extends beyond governments and private firms and ‘into individuals perceptions and responsibilities’ (*“Beta”*, 2004). During 2003 *Accenture* organized a major trans-American series of ‘citizens workshops’ on homeland security, concluding that ‘the people are the nation’s most important and untapped resource in the homeland security enterprise’ (*Council for Excellence*, 2004, p. 7). The subsequent report identifies information sharing and secure borders as citizens’ strategic priorities, suggesting that ‘well-intentioned Americans’ should volunteer their time to help fight the war on terror (p. 11). Yet, there are apparently no questions raised as to the implications of such citizen profiling for the Arab Americans and other groups who have found that risk profiling is racial and ethnic targeting (*Edley*, 2003; *Nagel*, 2002). As *Butler* (2004, p. 39) has put the problem, ‘when the alert goes out, every member of the population is asked to become a “foot soldier”’ in the war on terror, observing the behaviour of fellow passengers on a train, new neighbours in town, ‘and anyone who looks vaguely Arab in the dominant racial imaginary’. At the time of writing, in the wake of the July London bombings, the Chief Constable of London transport police is calling for increased vigilance on the part of commuters and tourists, simultaneously urging that stop and search powers should be ‘targeted’ and ‘should not waste time on white old ladies’ (*“Plan to Improve”*, 2005).

The making of the responsible and vigilant homeland security citizen is closely tied into the adventure and lifestyle gadgetry of smart phones and mobile hand-held technologies. Alongside the award of border control contracts to data and risk management companies, such firms also draw the citizen into the everyday armoury of the war on terror. A Seattle IT company, Town Compass LLC, for example, markets ‘personal products to fight the war on terror’. Their ‘Most Wanted Terrorists’ database is available as a free download to pocket PCs and smart phones as part of a ‘terrorism survival’ bundle. Town Compass promises that ‘people can have the photos and descriptions at their fingertips at all times in case they spot a suspicious person, easily comparing the person to the photo without endangering themselves’ (cited in *“Homeland Security Focus”*, 2004, p. 4). Should the vigilant citizen succeed in identifying a suspicious person, the download comes complete with one-touch dialing to the FBI and full details of currently available rewards. The electronically enabled citizen as foot soldier in the war on terror has similarly been called up (and into being) by the UK government following the London bombings. The ‘Life Savers’ hotline number is downloaded to mobile phones with the message that ‘people should consider whether the behaviour of those they encounter, through work or socially, gives them any reason to think they might be planning terrorist attacks’ (*Home Office*, 2005). In each of these cases the risk profiling and targeted governance that is writ large in the US VISIT programme establishes a new process of authorization, in which the everyday spheres of the commute, the office and the household become sites of authority in the war on terror.

For a politics of resistance or dissent, the problem of the growing ubiquity of the ‘homeland security citizen’ is one that appears to foreclose the possibility of public critique. Elsewhere I

have discussed in greater depth the problematic of resistance within the war on terror, suggesting that we find ourselves in ambivalent subject positions: both frequent flier and immigrant rights campaigner, for example; or both London city commuter and anti-war protester (Amoore, 2006). Though outside the scope of this article to pursue the resistance question further, I have argued that the looming presence of the biometric border should be taken seriously politically, but that it should also be destabilised and critiqued, perhaps made less serious, as in some of the examples of artistic interventions I have discussed.

I will suggest one example here, then, of an important and growing body of satirical readings of the making of the homeland security citizen. San Francisco animator, Mark Fiore, subjects the risk discourses of the Department of Homeland Security to observant political satire. In his short animation *Minister of Fear*, Fiore depicts Secretary Tom Ridge as the cloaked and masked ‘minister of fear’, bringing the risks of global terrorism to the living rooms of America. The *Minister* vacillates wildly between the calm assurance that the state has security in control: ‘remain calm, stand down, go about your business, code yellow’; and a screaming panic that warns ‘they are coming, look out! You never know where the terrorists might strike, they are coming... but in a non-specific and unsubstantiated way’.<sup>10</sup> In *Are you a Patriot?*, Fiore targets the Patriot Act’s explicit focus on citizens as surveillant individuals. The viewer is asked ‘to decide who should be investigated using the anti-terrorist Patriot Act’. The animation then shows a number of stereotyped mug shots, each time asking the viewer to decide: ‘suspected terrorist?; suspected pipe bomb nut?; suspected identity thief’.<sup>11</sup>

Rather as Heath Bunting’s works replay the dataveillance techniques of the war on terror, unsettling their apparently secure roots in science and law and rendering them incomplete and contingent, Mark Fiore unsettles the assumptions underpinning the making of the homeland security citizen. His short films serve to question the logics of profiling ‘suspicious behaviour’ and to repoliticise the homeland security discourses of risk and fear. We are left with the feeling that there is political significance in reclaiming uncertainty, in ‘accepting permanent uncertainty’, as Bigo (2001, 2002) puts it, and ‘learning to live’ with our fears. Indeed, as many writers have suggested, art, comedy and laughter have an important role to play in a politics that disrupts what we have come to see as necessary or normal ways of living (Bleiker, 2000; Odysseos, 2001). In the face of a war on terror that appeals to our sense of normal ‘ways of life’ and the ‘normal run of things’ (Johnson, 2002), satirical accounts such as Fiore’s serve to question what is seen as a normal way of life. If the daily commute, the workplace and the city street are to become domains of homeland security surveillance,<sup>12</sup> then a politics of dissent must begin from the point of unsettling their ubiquity and ordinariness, making them extraordinary and open to question.

### Conclusions: life and death at the biometric border

I have argued that the biometric border signals a dual move in the contemporary politics of the war on terror: a significant turn to scientific and managerial techniques in governing the mobility of bodies; and an extension of biopower such that the body, in effect, becomes

<sup>10</sup> For the full animation see [www.markfiore.com/animation/fear.html](http://www.markfiore.com/animation/fear.html).

<sup>11</sup> For the full animation see [www.markfiore.com/animation/areyou.html](http://www.markfiore.com/animation/areyou.html).

<sup>12</sup> Of course, in many ways this mode of surveillance is already underway. See, for example, Graham’s (2004) work on the city and surveillance in the war on terror.

the carrier of the border as it is inscribed with multiple encoded boundaries of access. At the time of writing, the response to the July 2005 London bombings suggests renewed political fervour for the biometric border in the UK, with proposed new terror laws encompassing biometric immigration cards and calls for an acceleration of the US VISIT style European e-borders programme. As in the opening citation of this article, the response to the London attacks has indeed been that ‘there ought to be a way of solving any problem through science and law’.

Yet, it is in the tragic death of Brazilian immigrant, Jean Charles de Menezes, killed by police officers engaged in the more ‘old fashioned’ stake-out surveillance of a block of flats, that we find some of the most stark political implications of risk profiling in the war on terror. In the aftermath of the Metropolitan Police’s admission that they had mistakenly shot dead Mr. de Menezes on Stockwell underground station in the course of their anti-terror operations, the debate turned to questions of identity, status and profiling. In effect, once it became clear that de Menezes could not be represented as the terrorist embodiment of bare life, a struggle began to reposition his ‘otherness’ as that of the illegal immigrant. The discovery that Jean Charles’ student visa may have expired two years previously led to questions surrounding his ‘legality’. Disputes emerged as to whether or not he was ‘wearing a bulky jacket’ in hot weather or had ‘jumped the ticket barrier’ (*“Brazilian Did”*, 2005) – presumably seen as profiles of suspicious behaviour that may have led the officer to shoot to kill. In the moment of the decision to shoot to kill we see something of the logic of the profiling of suspicious behaviour that underpins the logic of the biometric border. The distinction, though, is that (despite lost CCTV footage that could have, paradoxically, exposed his ‘normal’ gait and denim jacket and his use of the frequent traveller’s Oyster card), this killing of Homo Sacer is visible in a way that the multiple deaths that will undoubtedly occur at the biometric border are not. When the integrated databases of US VISIT reach a moment of decision based on patterns of behaviour, these will not be in public view, even to the limited extent that de Menezes’ death is visible. The biometric border envisages drawing a clear, clean and unambiguous line between legitimate/low risk and illegitimate/high risk mobilities (a line that cannot be drawn, but is always in process of being drawn). Within the logic of the biometric border, the immigrant risks, in an acute and absolute sense, being profiled as a terrorist, particularly if he has no papers.

De Genova (2002, p. 436) has depicted the border as ‘the exemplary theatre for staging the spectacle of the “illegal alien” that the law produces’. Within the war on terror, the biometric border is, at least potentially, staging that spectacle on the railway platform, the subway, the city street, the vehicle license bureau, and so on. Read in this way the border becomes a condition of being that is always in the act of becoming, it is never entirely crossed, but appears instead as a constant demand for proof of status and legitimacy. The biometric border performs something, then, of Agamben’s (1998, p. 8) ‘bare life’ in which living is reduced to calculability, to the ‘life of homo sacer... who may be killed and yet not sacrificed’. The establishment of verifiable identity at the biometric border thus becomes a condition of being, in the sense of living within a particular society or way of life, if not indeed a condition of life itself.

I have argued throughout this paper that the biometric border implicates us all in the governing of mobility and in the profiling of suspicious behaviour. It does so via the promise of happiness and security and a world rid of ambiguity and uncertainty. The war on terror not only separates ‘our war’ from ‘their terror’, but also ‘our globalization’ of legitimate and civilized business and leisure travel from ‘their globalization’ of trafficking and illegal migration. The distinction is, of course, a feigned divide. Consider, for example, the many ways in which the category of migrant illegality actively supports the ‘legitimate’ worlds. Buried in the

newspaper reports of Jean Charles de Menezes' death was the background information that he had been working as a contract electrician and, the night before the shooting, as a night porter in a London hotel. Where the biometric border promises invulnerability through the risk profiling of categories of people, we might begin our critique by reflecting on the ways in which the low risk practices of our daily lives are wrapped up in the high risks borne in the lives of others.

## Acknowledgements

I thank the participants at those events for their comments. I wish to thank Marieke de Goede, Jenny Edkins, Paul Langley, April Biccum, Maja Zehfuss and Heath Bunting, and the three anonymous reviewers for their interventions. Sincere thanks to the immigration lawyers, privacy advocates and consultants who have given, so generously, their time. I acknowledge the financial support of the British Academy in the research and preparation of this article.

## References

- Accenture digital forum. (2004). US DHS to develop and implement US VISIT program at air, land and sea ports of entry. <[www.digitalforum.accenture.com](http://www.digitalforum.accenture.com)>.
- Accenture hits the daily double. (2004). *Business Week*, 3891, 74.
- Accenture press release. (2004). Government security contract to help make US safer. <[www.carers3.accenture.com/careers/global.aboutaccenture/careersnews/cn-usvisit](http://www.carers3.accenture.com/careers/global.aboutaccenture/careersnews/cn-usvisit)>.
- Agamben, G. (1998). *Homo Sacer: Sovereign power and bare life*. Palo Alto, CA: Stanford University Press.
- Agamben, G. (2005). *State of exception*. Chicago: University of Chicago Press.
- Amoore, L. (2004). Risk, reward and discipline at work. *Economy and Society*, 33(2), 174–196.
- Amoore, L. (2006). There is no great refusal: The ambivalent politics of resistance. In M. de Goede (Ed.), *International political economy and poststructural politics*. Basingstoke, UK: Palgrave.
- Amoore, L., & de Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change*, 43(2), 149–173.
- Appadurai, A. (1996). Number in the colonial imagination. In A. Appadurai (Ed.), *Modernity at large*. Minneapolis: University of Minnesota Press.
- Baker, T. (2002). Liability and insurance after September 11: Embracing risk meets the precautionary principle. *University of Connecticut School of Law Working Paper Series*.
- Baker, T., & Simon, J. (Eds.). (2002). *Embracing risk: The changing culture of insurance and responsibility*. Chicago, IL: University of Chicago Press.
- Beta (2004, August). *CIO Insight*, 42, 22.
- Bhabha, H. (1994). Frontlines/borderposts. In A. Bammer (Ed.), *Displacements: Cultural identities in question*. Indianapolis: Indiana University Press.
- Bigo, D. (2001). The Möbius ribbon of internal and external security(ies). In M. Albert, D. Jacobson, & Y. Lapid (Eds.), *Identities, borders, orders: Rethinking international relations theory*. Minneapolis: University of Minnesota Press.
- Bigo, D. (2002). To reassure and to protect: After September 11. *Social Science Research Council essay archive*. <[www.ssrc.org/sept11/essays/bigo.htm](http://www.ssrc.org/sept11/essays/bigo.htm)>.
- Biometrics: Great hope for world security or triumph of big brother? (2004, June 18). *The Guardian*, 17.
- Billions misspent in post September 11 anti terror buying. (2005, May 8). *New York Times*, A4.
- Bleiker, R. (2000). *Popular dissent, human agency and global politics*. Cambridge, UK: Cambridge University Press.
- Brazilian did not wear bulky jacket. (2005, July 28). *The Guardian*. <[www.guardian.co.uk/uk\\_news/story/0,,1537457,00.html](http://www.guardian.co.uk/uk_news/story/0,,1537457,00.html)>.
- Butler, J. (1997). *Excitable speech: A politics of the performative*. New York: Routledge.
- Butler, J. (2004). *Precarious life: The powers of mourning and violence*. London: Verso.
- Butler, J., Laclau, E., & Zizek, S. (2000). *Contingency, hegemony, universality: Contemporary dialogues on the left*. London: Verso.

- Clarke, R. (1994). Dataveillance: Delivering 1984. In L. Green, & R. Guinery (Eds.), *Framing technology: Society, choice and change*. London: Routledge.
- Connolly, W. (2005). *Pluralism*. Durham and London: Duke University Press.
- Council for Excellence. (2004). We the people: Homeland security from the citizens' perspective. Council for Excellence in Government in association with Accenture.
- Coutin, S. B. (2000). *Legalizing moves: Salvadoran immigrants' struggle for US residency*. Ann Arbor: University of Michigan Press.
- Coutin, S. B., Maurer, B., & Yngvesson, B. (2002). In the mirror: The legitimation work of globalization. *Law and Social Inquiry*, 27(4), 801–843.
- Cunningham, H., & Heyman, J. M. (2004). Mobilities and enclosures at borders. *Identities: Global Studies in Culture and Power*, 11(3), 289–300.
- Dear, M., & Lucero, H. M. (2005). Postborder cities, postborder world: The rise of Baja California. *Environment and Planning D: Society and Space*, 23, 317–321.
- De Genova, N. P. (2002). Migrant illegality and deportability in everyday life. *Annual Review of Anthropology*, 31, 419–447.
- De Goede, M. (2003). Hawala discourses and the war on terrorist finance. *Environment and Planning D: Society and Space*, 21(5), 513–532.
- De Goede, M. (2004). Repoliticising financial risk. *Economy and Society*, 33(2), 197–217.
- De Goede, M. (2005). Carnival of money: Politics of dissent in an era of globalizing finance. In L. Amoore (Ed.), *The global resistance reader* (pp. 379–391). London: Routledge.
- Department of Homeland Security. (2004). Transcript of Secretary of Homeland Security Tom Ridge at the Center for Transatlantic Relations at Johns Hopkins University. <<http://www.dhs.gov/dhspublic/display?theme=44&content=3994&print=true>>.
- Department of Homeland Security. (2005). Remarks by Secretary of Homeland Security Tom Ridge at the European Policy Centre. <<http://www.dhs.gov/dhspublic/display?content=4293>>.
- Dillon, M. (2002). Network society, network-centric warfare and the state of emergency. *Theory, Culture and Society*, 19(4), 71–80.
- Dillon, M. (2004). The security of governance. In W. Larner, & W. Walters (Eds.), *Global governmentality: Governing international spaces*. London: Routledge.
- Dillon, M., & Reid, J. (2001). Global governance, liberal peace and complex emergency. *Alternatives*, 25(1), 117–143.
- Dreyfus, H., & Rabinow, P. (1983). *Michel Foucault: Beyond structuralism and hermeneutics*. Chicago: University of Chicago Press.
- Edley, C. (2003). The new American dilemma: Racial profiling post-9/11. In R. Leone, & G. Anrig (Eds.), *The war on our freedoms: Civil liberties in an age of terrorism*. New York: Public Affairs.
- Ewald, F. (1991). Insurance and risk. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in governmentality*. Chicago: University of Chicago Press.
- Foucault, M. (1976). *The will to knowledge*. In: *The history of sexuality, Vol. 1*. London: Penguin.
- Foucault, M. (1983). Afterword: The subject and power. In H. L. Dreyfus, & P. Rabinow (Eds.), *Michel Foucault: Beyond structuralism and hermeneutics*. Chicago: University of Chicago Press.
- Graham, S. (Ed.). (2004). *Cities, war and terrorism: Towards an urban geopolitics*. Malden, MA: Blackwell.
- Gregory, D. (2004). *The colonial present*. Oxford: Blackwell.
- Heimer, C. (2002). Insuring more, ensuring less: Private regulation through insurance. In T. Baker, & J. Simon (Eds.), *Embracing risk: The changing culture of insurance and responsibility*. Chicago: University of Chicago Press.
- Home Office (2005). *Terrorism: What you can do*. London: HMSO.
- How to cross borders, social or otherwise: Art Project could be a security nightmare. (2004, October 27). *New York Times*, A48.
- Homeland security focus. (2004). *Military and Aerospace Electronics*, 15(7), 4.
- Hyndman, J. (1997). Border crossings. *Antipode*, 29(2), 149–176.
- Johnson, R. (2002). Defending ways of life: The (anti-) terrorist rhetorics of Bush and Blair. *Theory, Culture and Society*, 19(4), 211–231.
- Kestelyn, J. (2002). For want of a nail. *Intelligent Enterprise*, 5(7), 8.
- Larner, W., & Walters, W. (Eds.). (2004). *Global governmentality: Governing international spaces*. London: Routledge.
- Levi, M., & Wall, D. S. (2004). Technologies, security, and privacy in the post-9/11 European Information Society. *Journal of Law and Society*, 31(2), 194–220.
- Lyon, D. (2003a). *Surveillance after September 11*. London: Polity.
- Lyon, D. (Ed.). (2003b). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. New York: Routledge.

- Lyon, D., (2004). Identity cards: Social sorting by database. (OII Issue Brief no.3).
- Nagel, C. (2002). Geopolitics by any other name: Immigration and the politics of assimilation. *Political Geography*, 21(8), 971–987.
- Newman, D. (2001). Boundaries, borders and barriers: Changing geographic perspectives on territorial lines. In M. Albert, D. Jacobson, & Y. Lapid (Eds.), *Identities, borders, orders: Rethinking international relations theory*. Minneapolis: University of Minnesota Press.
- Odysseos, L. (2001). Laughing matters: Peace, democracy and the challenge of the comic narrative. *Millennium: Journal of International Studies*, 30(3), 709–732.
- O'Malley, P. (2000). Uncertain subjects: Risks, liberalism and contract. *Economy and Society*, 29(4), 460–484.
- Plan to improve relations with Muslim communities. (2005, August 1). *The Guardian*, 8.
- van der Ploeg, I. (2003). Biometrics and the body as information: Normative issues of the socio-technical coding of the body. In D. Lyon (Ed.), *Surveillance as Social Sorting*. London: Routledge.
- Rose, N., & Valverde, M. (1998). Governed by law? *Social and Legal Studies*, 7(4), 541–551.
- Rules of crime. (2004). *New Museum of Contemporary Art*. <[www.newmuseum.org](http://www.newmuseum.org)>.
- Salter, M. (2003). *Rights of passage: The passport in international relations*. Boulder, CO: Lynne Rienner.
- Schneider, F. (2002). *BorderXing guide: Reverse authentication*. London: Tate Modern.
- The price of protecting the airways. (2001). *Business Week*. <[www.businessweek.com/print/technology/content/dec2001/tc2001124\\_0865.htm](http://www.businessweek.com/print/technology/content/dec2001/tc2001124_0865.htm)>.
- Thrift, N. (2004). Movement–space: The changing domain of thinking resulting from the development of new kinds of spatial awareness. *Economy and Society*, 33(4), 582.
- US House of Representatives. (2002). Helping federal agencies meet their homeland security missions: How private sector solutions can be applied to public sector problems. Testimony transcript, February 26. Washington, DC: Subcommittee on Technology and Procurement.
- Valverde, M., & Mopas, M. (2004). Insecurity and the dream of targeted governance. In W. Larner, & W. Walters (Eds.), *Global governmentality: Governing international spaces*. London: Routledge.
- Van Munster, R. (2004). The war on terrorism: When the exception becomes the rule. *International Journal for the Semiotics of Law*, 17, 141–153.
- Walters, W. (2002). Mapping Schengenland: Denaturalizing the border. *Environment and Planning D: Society and Space*, 20, 561–580.