Crime, Law & Social Change (2005) 43: 149–173
DOI: 10.1007/s10611-005-1717-8

Governance, risk and dataveillance in the war on terror

LOUISE AMOORE and MARIEKE DE GOEDE*
University of Durham, UK and University of Amsterdam, Amsterdam, The Netherlands;
**author for correspondence (e-mail: m.degoede@uva.nl)*

Abstract. This paper critically analyses the importance of risk management techniques in the war on terror. From the protection of borders to international financial flows, from airport security to daily financial transactions, risk assessment is emerging as the most important way in which terrorist danger is made measurable and manageable. However, we argue that the risk-based approach results in the displacement of risk onto marginal groups, while its effectiveness in the war on terror remains questionable.

"Mathematics provides a whole new set of tools in the war on terror."

(Gordon Woo, Risk Management Solutions, 2004)

"Every day we must operate with the knowledge that our enemies are changing based on how we change. That is why science and technology is key to winning this new kind of war."

(Tom Ridge, US Secretary of Homeland Security, 2005)

Introduction: Terrorist risk

According to Gordon Woo of the London-based firm Risk Management Solutions (RMS), mathematical risk assessment models are important policy tools in the war on terror, because they provide an understanding of, for example, "how terrorists select targets" as well as "the chances. . .of disrupting a terrorist network." According to Woo, terrorists "are being entirely rational in optimizing their own particular objectives. And their extremism, their absolutism in reaching their goals, actually makes it easier to use these mathematical models." The risk models developed by RMS help allocate security budgets by identifying vulnerable places and suspicious people. It is in this sense, according to Woo, that "mathematics provides a whole new set of tools in the war on terror" (quoted in Theil, 2004).

This article critically analyses the importance of risk management techniques in the war on terror. From the protection of borders to international financial flows, from airport security to daily financial transactions, risk assessment is emerging as the most important way in which terrorist danger is made measurable and manageable. For criminologists, this development is nothing

new but takes place within a larger shift towards what Mariana Valverde and Michael Mopas call 'targeted governance.' The new penology, according to Valverde and Mopas (2004: 240), involves a "shifting away from discipline to risk. Discipline. . .governs individuals *individually* while simultaneously forming and normalizing populations. Risk management, by contrast, breaks the individual up into a set of measurable risk factors" (emphasis in original). The new emphasis on risk in penology combines a neoliberal disappointment in welfare-state objectives of totalizing transformations with an optimistic belief in the ability of information and technology to produce a risk-free society. Targeted governance entails a limited and risk-driven intervention into society, based upon a "dream" of a "'smart,' specific, side-effects-free, information-driven utopia of governance" (Valverde and Mopas, 2004: 239).

It should be clear that this paper does not suggest that post-9/11 risk management is entirely new, nor that it operates with full reach and consistency. For example, there is a rich literature critically examining border policing prior to 9/11 (for example Bigo, 2002; Doty, 2003; Andreas and Snyder, 2000). In fact, we have written about the politics of risk management discourses in finance and consulting that were clearly visible before 9/11 (Amoore, 2004; de Goede, 2005). Moreover, the risk management practices discussed here continue to face substantial bureaucratic and political resistance, and unevenness of application. However, it is perhaps precisely because of the political resistance to targeted governance that the representation of 9/11 as a radical break with the past was able to accelerate the risk management programs that predate the attacks. The idea that a radically new threat demands a radically new response was able to generate political support for controversial data-mining programmes (O'Harrow, 2005). In addition, what is new about contemporary terrorist risk management, as the article discusses, is its increasing reliance on technology and computerised data-mining. Inside data-mining technology, questionable data become hardened facts – making critical political analysis of these practices warranted.

Valverde and Mopas' concept of targeted governance, then, is highly pertinent to analysing developments in the war on terror, for two reasons. First, it offers an understanding of dispersed power, "in which the state is not a necessary or logical centre" (Larner and Walters, 2004: 4). In the war on terrorism, it is important to understand how power is exercised through a complex policy constellation including regulatory state bodies, international institutions, industry self-regulating bodies and private risk assessment firms. This does not simply entail a shift from public to private authority, but entails more precisely the enduring and even enhanced power of particular state agencies, in close cooperation with international institutions and private risk assessment firms.

Secondly, the concept of targeted governance focuses in some empirical detail on the "acts, tactics and practices of governing" (Larner and Walters, 2004: 4). In other words, it becomes important to study the practical and technical manifestations of targeted governance, and in particular the risk assessment models designed by Gordon Woo and others. Perhaps the main aspect of these risk assessment models is what Mike Levi and David Wall (2004: 200), following Roger Clarke et al. (1994), call *dataveillance*, or "the proactive surveillance of what effectively become suspect populations, using new technologies to identify 'risky groups'". The war on terror involves the classification, compilation and analysis of data on, for example, passenger information and financial transactions on an unprecedented scale. These techniques of governance rely heavily on sophisticated computer technology and complex mathematical modelling to mine data and single out suspicious behaviour.

It should not be forgotten that risk management in the war on terror is not only a technique of governance, but also a profitable industry. As David Lyon (2003a: 47) has put it, "these places of high risk as danger [airports, borders] are also places of high risk as economic adventure." This article analyses risk as danger and economic opportunity in two distinct areas of the war on terror: the policing of the movement of money, and the movement of people.[1] In both cases we are concerned to draw out the consequences of techniques of dataveillance-driven risk management for vulnerable groups. The first part of the paper examines the war on terrorist finance, and discusses how the scrutiny of financial data has become inscribed with a preventative function in the fight against terrorism.[2] We assess the social consequences of the financial fight against terrorism, that may include financial exclusion, especially of migrant groups. In the second part we discuss the extension of risk management into border controls via a focus on the US VISIT programme. We are concerned with US VISIT as a set of techniques for regulating mobility, in which private risk experts are authorised to identify and target risky persons. The conclusion draws together these two areas in order to reflect upon the wider meaning of risk, governance and dataveillance in the war on terror.

The risk of terrorist financing

In the war on terrorist financing the new risk-based approach that is currently being developed by governments and international institutions, can be said to constitute a practice of targeted governance. The war on terrorist financing includes a bewildering amount of new regulation, directives and best practice guides from a diversity of institutions, including the US Treasury, the

International Monetary Fund (IMF), the United Nations (UN), and the Financial Action Task Force (FATF). What is emerging at the heart of this policy constellation is a risk-based approach, focused on the collection and analysis of financial data in order to identify suspicious transactions that may indicate terrorist behaviour. The Financial Crimes Enforcement Network (FinCen) of the US Treasury, for example, collects and analyses suspicious action reports (SARs) filed by diverse financial institutions – which may lead to criminal prosecution. FinCen has existed since 1990 but its tasks have been significantly expanded under the Patriot Act, and the agency has subsequently pursued around 500 cases. "Our approach to regulation is risk-based," declared FinCen's director William J. Fox (2004a) in a recent speech, "we believe effective implementation of [anti-money laundering law] must be predicated upon a financial institution's careful assessment of its own vulnerabilities to money laundering and other financial crime. . ..It is not a 'rule-based' approach, where the regulator gives the regulated a laundry list to be checked off."

At the heart of FinCen's strategies and policies is the (contestable) conviction that follow-the-money techniques are effective in identifying and comprehending not just the proceeds of crime – but also in assessing the *intentions* of terrorists, who may need to be apprehended *before* they commit their crimes. In other words, money laundering regulation is evolving from a regulatory tool designed to confiscate criminal money after the act (with a desired deterring effect) to a regulatory tool required to predict and apprehend potential terrorists. In its preoccupation with risk assessment and prediction, the war on terrorist finance represents a marked break with earlier regimes of money laundering regulation, which focused on tracing criminal money – associated with narcotics or political corruption – *after* the crime.[3] If undermining crime and amassing evidence were the objectives of pre-9/11 money laundering policy, predicting possible terrorist attacks became the objective after 9/11 (Malkin and Elizur, 2002: 64). For example, in a recent Hearing before the US House of Representatives, Fox (2004b) argued that "financial intelligence is actionable intelligence. It can...lead to effective strategic action that stops or disrupts the flow of money to terrorist and their networks, which, in turn, serves to *halt or impede terrorist operations*" (emphasis added).

The risk-based approach to terrorist financing entails the two aspects that according to Valverde and Mopas are particular to targeted governance. First, it is designed to reconcile the need for new financial regulation with the continuing operation of deregulated, neoliberal financial markets. This approach offers common ground to (inter)national public regulators and industry self-regulating bodies. It is designed, in part, to interfere minimally with existing global capital markets and offers profit opportunities to private

risk-assessment companies. As David Aufhauser (2003: 301–302), Chairman of the US National Security Council on Terrorist Financing, puts it: "The world economy is a deliberately open and porous one, designed to encourage the free flow of capital, investment and economic development. To elect rules that intrude on that dynamic is to hand victory to the enemy. . ..The measures that we champion in the war on terrorist financing are targeted to visit injury on the bankers of terror, not the engines of economic growth and prosperity." Secondly, the risk-based approach shares with targeted governance the utopia of smart, information-driven, financial risk management. The war on terrorist finance envisions the classification, compilation and analysis of financial transactions data on an unprecedented scale. Aufhauser (2003: 304) presents a vision of continuous computerised financial risk assessment capable of interrupting terrorist finance, through "the real time production of electronic commerce to a central storage facility."

Suspicious transactions

It is important to examine, however *what precisely* is deemed risky and suspicious in the emerging policy constellation that pursues the war on terrorist finance. For example, according to US Treasury's *Terrorist Financing Rewards Program*, which offers rewards of up to US$ 5 Million for "information leading to the dismantling of any system used to finance a terrorist organization," suspicious transactions include: "account transactions that are inconsistent with past deposits or withdrawals," "transactions involving a high volume of incoming or outgoing wire transfers" and "wire transfers by charitable organizations to companies located in countries known to be bank or tax havens."[4] This rewards program has distributed posters and flyers with classifications of suspicious transactions accompanied by images of Osama bin Laden and the falling World Trade Towers, in order to urge the public to report "possible illegal financial activity." It thus encourages what Lyon (2003a: 59) calls a "culture of suspicion," in which ordinary citizens are called upon as "the eyes and ears of police and intelligence." The Rewards program emphasises foreign wire transfers as a source of suspicion and identifies as 'illicit sources' welfare and food-stamp fraud, cigarette smuggling, counterfeit merchandise and alternative remittance systems. But the representation of terrorist money as a 'foreign problem,' and the enumeration of a host of misdemeanours such as welfare fraud and counterfeit merchandising under the terrorist banner is very problematic (also Campbell, 2004).

However, even more significant than the Rewards Programme, because operating with further reach and consistency, is the move towards computerised

financial data-mining that aims to reduce terrorist danger while presenting a commercial opportunity. Private data mining companies, including the British data mining companies Mantas and World-Check, develop software tools to be used by financial institutions to single out suspicious transactions and – perhaps even more importantly – ensure regulatory compliance. This software relies on modelling patterns of normality in order to identify deviations from the norm. "We know the profile of every dairy producer, every butcher, every teacher," says one software developer for Mantas, "and that becomes important in money laundering as many businesses operate as a front for money laundering and banks will need to [look] at how that type of business normally behaves" (Mantas, 2003).

The fact that risk-technology is computerised, moreover, is not incidental to its power but at the heart of it. Unlike the Rewards programme which relies on public tip-offs, Mantas classifications operate more consistently and more powerfully by virtue of being institutionalised and computerised. Software, according to Bowker and Star, is a 'frozen organisational discourse' because the "arguments, decisions, uncertainties and processual nature of decision-making are hidden away inside a piece of technology. . ..Thus values, opinions and rhetoric are frozen" (quoted in Leyshon and Thrift, 1999: 441). In other words, all doubts and discussion concerning what constitutes terrorist financing and how to track it – a discussion which is ongoing (see for example Passas, 2004a,b; Pieth, 2002) – is silenced inside Mantas's models. "Software installs relatively unchangeable, taken-for-granted protocols in the day-to-day information practices of organizations, providing unified ways of interpreting events, influencing the ways in which decisions are made and standardizing such decisions over time and space," Leyshon and Thrift (1999:453) conclude.

Financial exclusion

In the risk classifications designed to trace terrorist financing, then, certain *suspicious people* and *suspicious places* are identified. It stands out that those without regular income and expenditure, as well as those who send international wire transfers in small amounts, are considered especially suspect. This includes, most notably, migrant, students, and the unemployed. Perhaps this is not odd, given that the September 11 hijackers pretended to be students while living in the US prior to their attack. However, political criticism *must* raise the question whether criminalising large groups at the margins of society can have a preventative function in the war on terrorist finance. Here, we draw out three areas of concern where the war on terrorist finance is transforming not just the international financial architecture, but the *everyday life of global finance*

(Langley, 2002). First, the war on terrorist finance is exacerbating financial exclusion, through more stringent 'Know-Your-Customer' (KYC) regulation in retail finance. Second, the war on terrorist finance is affecting particularly hard migrant communities and their possibilities to send remittances. Third, *cash itself* is becoming increasingly suspect and an explicit objective of the war on terrorist finance is the reduction of cash use.

First, there is evidence that increased KYC regulation in retail banking may exacerbate financial exclusion. KYC, simply, requires banks to hold formal proof of identification and residency of their customers, and may also include information on the "purpose and reason for opening the account"; "the anticipated level of activity" in the account; and the client's "sources of wealth and income" (FSA, 2003: 10–11). KYC, clearly, is not a new regulatory directive, but what is new since the 9/11 attacks is its relevance for retail finance. Before 9/11 money laundering risk was assumed to be associated with certain transactions thresholds. However, the relatively small amounts needed by Atta and his accomplices has refocused money laundering control and terrorist financing measures on the daily life of retail finance. In Britain for example, the 'Fighting Crime and Terrorism: We Need Your Help' campaign launched in mid-2003, requires high-street banks to step up security checks not just of new retail customers, but also of existing ones. The campaign leaflets compel banking clients to comply with the new identification requirements under the banner "You can make life harder for terrorists," and lists the acceptable identification documents, including passport and proof of residency.[5] However, as a critical investigation in *The Guardian* points out, it is not uncommon for poorer population groups to have neither passport nor driver's license, while tenants do not always have proof of residency in the form of utility or council tax bill. *The Guardian* concludes: "All banks say they can be flexible on identity requirements. But counter staff are often rigid in interpreting rules, scared of disciplinary action if they make a mistake" (Levene, 2003: 3). While KYC rules make sense in an institutional setting that has harboured the money of corrupt dictators like Abacha (Malkin and Elizur, 2001: 21–22) they are questionable in the context of high-street retail finance.

In developing countries the problems surrounding KYC regulation may be even more acute, as is demonstrated by a recent report of South Africa's FinMark Trust, which promotes financial inclusion of the poor. New KYC rules required by Financial Action Task Force (FATF) are very difficult to implement in a country where "one third of the population live in informal dwellings without formal address whilst up to half of the population lack the documents to verify their residential address" (Bester et al., 2004: ii). Post-apartheid South Africa is keen to reintegrate in the international community,

and regards implementing anti-money laundering regimes as part of this effort. Moreover, effects of non-compliance can be serious, as Bester et al. (2004: 4) note, and "can impact negatively on the economy of a country." However, KYC regulation leaves South Africa's banks in a double bind: *either* they contravene the law, *or* they are forced to exclude from banking facilities clients from relatively poor and mobile constituencies who do not hold the necessary documents – thus contravening national policies which seek to increase financial inclusion. FinMark concludes that the international community needs to allow a flexible interpretation of rules, particularly for developing countries. However, South Africa has already come under FAFT criticism for allowing exemptions to KYC requirements, and the case thus demonstrates the pressure that countries are under to ensure compliance with new anti-terrorist financing regulation.

Secondly, the war on terrorist finance is having a profound impact on the opportunities that migrants have to send remittances. As one of us has argued elsewhere, 'hawala,' or informal money transfer networks, have received excessive scrutiny in the wake of September 11 for being a conduit for terrorist financing and have been needlessly criminalised (de Goede, 2003). To be sure, there is now increasing recognition of the developmental potential of remittances *and* increasing recognition of the important role that informal money transfer networks play. Evidence of the positive role of informal transfer networks is growing, and it is pointed out that these offer relatively cheap and reliable channels for remittances to (rural) areas where Western banks may not be present (for example, Al-Suhaimi, 2002; Horst and van Hear, 2002; Maimbo, 2003).

At the same time however, the criminalisation and suppression of informal money transfer networks continues. The FATF's Eight Special Recommendations on Terrorist Financing calls for the regulation and registration of alternative remittance systems, and the implementation of KYC regulation.[6] The Patriot Act, similarly, calls for "routine record keeping and reporting" of informal money transfers, including verification of customer identity (US Department of the Treasury, 2002: 7–8). These requirements seem reasonable. But although informal remittance operators in all probability *know* their clients on a more personal level than high street banks do, producing the official documents specified under KYC regulation may be problematic, especially, of course, for undocumented migrants. While informal money transfer networks have been widely vilified for 'leaving no paper trail,' it is more accurate to say that they do engage in extensive record keeping and KYC practices, but in manners that are not recognised by Western regulatory requirements.

Informal remittance networks, moreover, continue to be singled out as suspect and especially suitable for channelling terrorist money. For example,

a paper published by the Harvard Law School's Seminar on International Finance in April 2002 attributes the continuing existence of informal money transfer networks to "the benefits they offer for illicit finance," and links them to "narcotics, trafficking in human beings, terrorism, corruption, and smuggling" (Gillespie, 2002: 8–9). Moreover, the US Treasury's National Money Laundering Strategy identifies alternative remittance systems as "particularly vulnerable or attractive to terrorist financiers and money launderers" (US Department of the Treasury, 2003: 13).

Criminalisation in policy discourse has very real material effects, and it is important to note that among the few actual convictions under the Patriot Act are a number of imprisoned and fined unlicensed money remitters. The 2003 Money Laundering Strategy notes that "the United States has succeeded in disrupting the operations of several illegal money remitters *potentially* implicated in terrorist financing" (US Department of the Treasury, 2003: 15, emphasis added). More specifically, FinCen's 2002 report to Congress details a number of cases where informal remittance networks have been prosecuted, including two cases of unlicensed hawalas sending remittances to East Africa, and the imprisonment of an unlicensed Boston hawaladar (US Department of the Treasury, 2002: 30, 36, 38). However, the Patriot Act "specifically provides that a conviction for failure to comply with a state licensing requirement does *not* need to require proof that the defendant knew of the state licensing requirement." This means that hitherto condoned or invisible money remitters found themselves prosecuted after September 11 for failing to have acquired licenses of which they may not have known.

My point here is not that informal money remitters are *never* involved in criminal activity, but more precisely to question the identification of hawala as especially suspect and vulnerable to abuse. As Passas (1999: 67) concludes in his report to the Dutch Ministry of Justice, informal value transfer systems "do not represent a money laundering or crime threat in ways different from conventional banking or other legitimate institutions" (see also Passas, 2004a,b). This point is supported by the report of the 9/11 Commission, that is especially harsh in its condemnation of the actions that the Bush administration took against the large Somali-based money remitter al-Barakaat. Al-Barakaat was considered suspicious for remitting large amounts of cash from the US-based Somali Diaspora back to Somalia and was closed down by the Bush administration in November 2001 – at which time Kenneth Dam of US Treasury claimed to have disrupted millions of dollars destined for terrorist organisations. However, the 9/11 Commission concludes that despite "unparalleled access and support" from the central bank of the United Arab Emirates, which made available thousands of pages of documents related to al-Barakaat accounts, they found *no* evidence linking al-Barakaat to terrorist

activity, and "no evidence that closing the al-Barakaat network hurt al-Qaeda financially" (Roth et al., 2004: 81). The Commission suggests that poor understanding of remittances and prejudice against migrants may underlie the harsh pursuit of al-Barakaat, because criminal authorities assumed fraud *must* be at work when they discovered the amounts of money remitted by the Somali migrant community of Minneapolis to their home country (Roth et al., 2004: 74). The report further notes the damage done to Somali migrants when their remittances were frozen and not delivered to the intended recipients.

It is difficult not to conclude that pursuing unlicensed money remitters offers FinCen an easy target and allows it to report success to Congress, while its effect on preventing terrorist financing remains dubitable. Meanwhile, migrants are deprived of relatively cheap and efficient ways of sending money to their families, and are increasingly dependent on more expensive formal channels like Western Union.

Thirdly, cash itself is becoming increasingly suspect, and the war on terrorist finance has an explicit goal to reduce the use of cash worldwide. The objective of reducing cash use is not new, and the FATF's 40 Anti-Money Laundering Recommendations, published in 1990, include the stipulation that "Countries should. . .encourage. . .the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book entry recording of securities, as a means to encourage the replacement of cash transfers."[7] But the political significance of reducing cash use increases in the context of dataveillance, as it expands further into the realm of everyday finance. Surveillance technology in the risk society relies on "the proposition that each movement or transaction. . .leaves a trail of electronic traces, which means that individuals cannot easily disappear" (Levi and Wall, 2004: 206). In other words, money in electronic form – credit cards, account debits, ATM transactions – is registered and traceable, and thus police-able. At the heart of the policy pursued in the name of the war on terrorist finance is what Aufhauser (2003: 301) calls the *electronic footprint of the terrorists*: "People cannot plant themselves for years at a time in a foreign land without establishing a footprint of the source of their funding. . .. At some juncture – be it collection, recruitment, training, transport, housing, planning or execution – terrorist financing *will* intersect with the recorded financial system" (original emphasis).

However, the electronic footprint theory criminalises cash use, and ignores the growth of the informal economy that is not associated with criminal activity but with neo-liberal regimes of labour flexibility. If a sizeable informal economy was once seen as a sign of underdevelopment, it is now widely acknowledged that neo-liberal practices of global competition and labour flexibility have caused the growth of the informal economy in the centres of global

capitalism, and is inextricably connected to the exploitation of migrant labour (Peterson, 2003: 85–86; Sassen, 1991). A recent study on the US economy estimates that in California around 8 million illegal migrants work in the cash economy, and that in LA County about 28% of farm workers are paid in cash (Campbell, 2003). Migrant labour and informal employment are at the core – not the margin – of the contemporary global economy, and criminalising the cash economy implicates migrant labour in money laundering and terrorist financing. The criminal image of filthy lucre obscures the fact that many (migrant) workers have no choice but to depend on cash transactions in their daily lives, and that to some, cash can be "an anchor of materiality in a world of invisible wealth" (Appadurai, 2000: 643).

There is a fundamental contradiction at the heart of the war on terrorist finance, then. On the one hand, it is intended to control the risk of terrorist financing through hardening regulatory regimes such as KYC rules and the financial exclusion of certain suspect populations. On the other hand, KYC rules and the closing down of informal money transmitters may force – undocumented – migrants to turn to cash transfers and increases the informal economy. In fact, it is possible to argue that the contradictory policies produced by dataveillance underestimate the complexities of the task of cutting off terrorist financing. As Levi (2003: 118–119) concludes: "Instead of overly ambitious global 'data' and pattern estimates. . .it may be better to build up from the ground more modest analyses of what we can plausibly know about criminal money management." In addition, it is vital that migrant workers – even undocumented ones – are offered cheap and reliable opportunities for remitting money, and regulatory authorities would do well to require financial institutions to provide these.

Risk at the Border: US Visit and the Smart Border Alliance

In testimony before the US House of Representatives Subcommittee on Technology and Procurement in February 2002, a panel of management consultants and IT specialists argued that what had long been considered business problems were now posing a threat to US national security. In the discourses of the business world, what is known as the "stovepiping" of data – the isolation of information in singular and separate systems – is being highlighted as a key risk factor in the war on terror. "In this war", suggested the panel, "our enemies are hiding in open and available information" (cited in Kestelyn, 2002: 8). In the immediate months following the events of September 11, the dilemmas of the war on terror were being framed as problems of risk management or, more specifically, as uncertainties than can be resolved via

information technologies. As one CEO of a major management consultancy put it: "had information coordination technology been properly in place before September 11, there may have been a different outcome".[8] In evidence put to the House Subcommittee, management consultants and IT specialists made the case that the "preattack activities of the hijackers" could have been made visible to the authorities if they had not been hidden across a diverse range of databases. Had the databases been integrated and programmed with alertable suspicious patterns of behaviour, the experts argued, the threat could have been "identified and prevented" (cited in Kestelyn, 2002: 8).

As we have seen in the discussion of the theory of the "electronic footprint" left by terrorists in the financial system, at the heart of such programmes are "new ways of visualizing and governing deviant populations" that "juxtapose and synthesize the risk profiles generated by different tests" (Valverde and Mopas, 2004: 240). The use of technologies to produce and measure such risk profiles, a mainstay of corporate risk management strategies for over a decade, has entered the public sphere, bringing with it untold opportunities for profit in what is already being labelled a "homeland security market that has hit the big time" (Stein, 2004: 11). Three years on from the House Subcommittee hearing, the US Department for Homeland Security (DHS) named the *Smart Border Alliance*, headed up by management consultancy Accenture, as the primary contractor for a $ US 10 billion project, US VISIT.[9] The concept of US VISIT is to restructure and manage immigration systems at all US air, land and sea ports of entry, rendering the movement of people governable according to the logics of risk management. As Accenture itself defines the project:

> The end vision for the US VISIT solution is built around the concept of the virtual border. The virtual border is designed to operate far beyond US boundaries to help DHS assess the security risks of all US-bound travellers and prevent potential threats from reaching US borders (Accenture digital forum, 2004: 1).

Under the US VISIT programme the management of the border ceases to be a matter purely of geopolitical policing and discipline, in the sense of governing the entry and exit of peoples across mapped space, and becomes a matter of biopolitical management (Walters, 2002: 562). That is, the border becomes a "virtual" site through which the behaviours and daily practices of populations can be made amenable to intervention and management. We explore the US VISIT here as a further example of a bundle of risk management techniques that are emerging under the rubric of the war on terror. It offers a number of insights into the conjunction of targeted governance and dataveillance under the war on terror, but also represents but one small element of a raft of risk

management practices enabled by the US Patriot Act and making headway into the policy agendas of other western governments (Lyon, 2003b; Beeson, 2003). In the discussion that follows we will draw out the significance of US VISIT as: a) a system of risk management based on the "social sorting" of legitimate from illegitimate mobile persons; b) a set of dataveillance techniques that link information technology to a biometric 'anchor' in the human body; and finally c) a programme that actively authorizes private authorities and individuals to take part in policing the movement and conduct of people in their everyday lives.

Governing mobilities

Announcing his plans for the US VISIT programme to the European policy community, US Secretary of Homeland Security, Tom Ridge, highlighted the risks and rewards of living in a globalizing society. "As the world community has become more connected through the globalization of technology, transportation, commerce and communication", he explained, "the benefits of the global economy enjoyed by each of us are available to the terrorists as well" (Department of Homeland Security, 2005: 1). Framed in this way, the problem becomes one of isolating the legitimate transborder activities of the global economy, and segregating these from the illegitimate transnationalism of those who exploit the possibilities of open borders. As we have argued elsewhere, following Pat O'Malley and others, the discursive deployment of risk is closely allied to the representation of the risks and rewards of globalization (De Goede, 2004; Amoore, 2004; O'Malley, 2000). Far from seeking to minimize or limit the risks of a globalizing society, the new penology of targeted governance rests upon an "embracing of risk" made possible through the global integration of information technologies (Baker, 2002). The US VISIT system deploys just such an "embracing risk" approach, appearing to hold out the possibility of reconciling the image of porous international borders that are open for business, with the need for security at the border (Brisbin, 2004).

Accenture's "smart border solution" to the policing of international mobilities rests upon an electronic information-based system of risk management that engages in the "social sorting" of people into categories of riskiness (Lyon, 2003b). As the US business press succinctly capture Accenture's task:

> Half a billion foreign visitors cross America's borders, land at her airports, and dock at her harbors every year. Imagine trying to weed out the criminals

> and terrorists while keeping a track on everyone else as they vacation, conduct business, enrol in college – and try to drop out of sight once they've overstayed their visa. (Business Week, 2004a: 32).

The "weeding out" of criminals and terrorists from legitimate travellers is undertaken through the interfacing and integration of over 20 existing databases. Among the most significant are: IDENT, an automatic fingerprint identification system storing biometric data 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 US; IBIS, a "lookout" watch list interfaced with Interpol and national crime data; CLAIMS 3, holding information on foreign nationals claiming benefits; and an array of links to local law enforcement, financial systems and educational records. The integration of these searchable databases allows the authorities to profile and encode people according to degrees of riskiness.

Accenture's plans for computer assisted airline passenger profiling, for example, reject past systems of risk management that they say "can really only check the single person who is walking out to the plane". By contrast "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 Business Week, 2001: 1). As in the case of the surveillance of financial patterns of behaviour, the assumption is that encoded risk profiles can be used as a basis to predict future acts and behaviours. As David Lyon has put it, "the coded body or a person who attempts to cross a national border may find that she is already welcome or already excluded on the basis of an identity that is established by the codes" (Lyon, 2003b: 24).

It is precisely this predetermining and fixing of identities that is of central concern to privacy advocates, civil liberties organizations, and human rights groups. In April 2004 a coalition of such organizations, including the American-Arab Anti-Discrimination Committee, National Immigration Law Center, Electronic Privacy Information Center and American Civil Liberties Union, wrote to the Department of Homeland Security expressing their concern at the "enormous potential for error an violation of international human rights standards" in the US VISIT system.[10] Of particular concern was the open question of what happens to people who come up as "hits" on the various databases and how a "false hit" can be challenged. As one EPIC representative put the problem: "these technologies are assumed to provide a complete picture of who someone is – leaving people having to dispute their own identity".[11] In these terms the US VISIT system far exceeds Accenture's "recording" of entry and exit of non-US citizens and "matching"

of people to their travel documents and visas (Accenture digital forum 2004: 2). Rather, by encoding people with a pre-determined identity and assuming that high-tech identification process to be indisputable, 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 et al., 2002: 804). The risk management system sold to the US government, then, is more appropriately described as a risk displacement system. The virtual border envisaged by *Smart Border Alliance* and the Department of Homeland Security becomes actual in the lives of migrants who experience ever greater uncertainty in their lives. De Genova's reading of the US-Mexico border, for example, describes the border as the "exemplary theatre for staging the spectacle of the illegal alien" (2002: 436). US-VISIT leaves open the possibility of entrance to the US for non-business/ non-global economy travel, for example by Mexican workers, but with the proviso of the ongoing surveillance of Accenture's virtual border which will come into play in spheres from money and banking, to medical care, insurance and housing. The border thus becomes a mobile phenomenon that allows entry to the physical space of the US without offering open entrance to the social, political and legal space of the US. In a very real sense, the mastery of border risks by governments and their business and technology partners is undertaken on the back of the intensification and reallocation of risk onto the most vulnerable groups.

Biometrics and bodies

The deployment of electronic personal data in order to classify and govern the movement of people across borders can be captured under the rubric of dataveillance (Clarke et al., 1994). Yet the US VISIT programme extends the use of integrated personal data into biometrics, a move that signals what Levi and Wall have called a "new politics of surveillance" (2004: 194). The US Patriot Act introduced a set of practices for the use of biometrics that have become the technology standard for US VISIT. In effect the US VISIT system converges integrated databases with biometric identifiers such as electronic fingerprints, iris scans and facial recognition. Though the actual implementation of biometric identifiers has been beset with problems – leading the DHS to drop the requirement for biometric passports by October 2004, for example – the seductive allure of biometric data in the governance of mobility has taken a strong hold on public and private authorities (Forbes.com, 2004). The seduction comes from the human body being seen as an indisputable anchor

to which data can be safely secured. What Irma van der Ploeg has observed as a "gradually extending intertwinement of individual physical characteristics with information systems" (2003: 58), has served to deepen the faith in data as a means of risk management. "In a world of identity politics and risk management", argues David Lyon, "surveillance is turning decisively to the body as a document for identification, and as a source for prediction" (Lyon, 2001: 72).

In the US VISIT programme the use of biometric technologies as a source of identification and prediction is taking two important turns. The first is to seek to annex "low risk" travellers via the use of voluntary systems of biometric submission. As the Secretary of Homeland Security Tom Ridge explains:

> 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: 1).

Tom Ridge's participation in the US Air Transportation Association's 'Registered Traveller' project, which uses *Unisys* technology to link frequent fliers to a biometric database, suggests that biometrics is being used in a process of "risk pooling" (Heimer, 2002), whereby individuals classified in a similar risk category are grouped together for common treatment – in this case for swift passage through security checks. However, in populations targeted for higher risk pools the electronic connection of data to bodies is more invasive and the surveillance intensified. Regular commercial travellers across the Mexico–US border, for example, can submit biometric information in order to fast-track the security check point. Unlike Mr Ridge's frequent traveller card, however, the smart cards used at the US–Mexico border may be radio frequency identification enabled (RFID), making them, at least in theory, trackable within the US.

Such faith in the ability of biometric data to secure identity is playing a central role in the war on terror at the border. As exemplified by Mike Davis, director of FBI criminal justice services, when he informed a European conference of technology companies that "the only way to trace a terrorist is through biometrics", reassuring them that "we are obtaining DNA from terrorists around the world as we encounter them" (cited in *The Guardian*, June 18, 2004: 17). Leaving aside the question of the somewhat improbable nature of such a scenario, Mr Davis's belief that "the war on terror has come to rely on biometric technology" raises a number of questions. The first concerns

the purposes for which biometric data is collected and deployed. Despite assurances by the DHS that the US VISIT system will not be in breech of international privacy laws limiting access to personal data, it seems that biometric data systems are being traded precisely on the grounds that multiple agencies can have networked access. Western police and intelligence agencies have drawn up plans to share biometric information, such that US VISIT biometric requirements become a Trojan horse for their introduction elsewhere. As Accenture are keen to point out, "the US VISIT contract is a key win in a climate where other countries on the front line of terrorism are interested in similar programmes" (Accenture press release, 2004: 1). Plans in the UK to link a biometric ID card to US VISIT compliant passports, for example, suggest that there is a trend towards linking the governance of international mobility to national systems of biometric identification (Lyon, 2004).

Our second question concerns the representation of biometric technologies as infallible and unchallengeable verifiers of the truth about a person. The linking of biometrics to integrated databases not only appears to make the identification of a person beyond question, but also lends authenticity and credibility to all of the data that is connected to that identity. Treated as a scientific, neutral and "smart" solution to the problem of establishing identity, biometrics become discrete entities that can be parcelled up, contracted out, integrated, applied and innovated. Yet, rather than being a secure anchor to the human body, biometric technology represents an "informatization of the body," part of a process in which technologies are themselves incorporated into the bodily experience (van der Ploeg, 2003; see also Thrift, 2004). It is important, then, to challenge and destabilize the apparent security of the biometrics-body link, to point to the fallibility of technologies, as well as to the agency that is enacted as "technologies tend to take on a life of their own" (Levi and Wall, 2004: 204).

Authority and authorization

In their seminal discussion of the governmentalization of modern societies, Nikolas Rose and Mariana Valverde conclude that the "authority of authority" has been established and defended "through alliances between the different legitimacies conferred by law and expertise" (1998: 550). The US VISIT programme is just such a point of alliance between the law (embodied in the US Patriot Act) and expertise (conferred by the contracts with a range of risk management experts). On announcing Accenture's contract, the Department of Homeland Security argued 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" (DHS, 2 June, 2004a). Similarly, Accenture's Eric Stange, managing partner of the Homeland Security practice, talks of the *Smart Border Alliance* as "a strong team of highly qualified companies with significant border management expertise" (Accenture press release, 2004: 2). For one of Accenture's sub-contractors, Titan Corp., some of this expertise was acquired through the supply of interrogators and interpreters to the Abu Ghraib prison in Iraq.

Nonetheless, US VISIT represents a programme of authorization that actively decentres the state and blurs the boundaries of public and private domains of governance. By virtue of a system that disperses power throughout a network of agencies, the "surveillance of migrant illegality" (Coutin, 2000) takes a renewed twist that authorizes private authorities and individuals to engage in the everyday policing of the movement of people. According to reports of Accenture's bid for the US VISIT contract, for example, the consultants positioned immigrants at he heart of their proposals: "Accenture wowed government officials with a demo that included wireless tags that tracked immigrants whereabouts" (Business Week, 2004b: 74). Given US VISIT's status as a system designed to verify those who have visas (i.e. not for immigrants), it is this targeting of immigrant groups under the guise of efficient border management that is provoking widespread concern among civil liberties groups. As one civil liberties representative explained: "since 9/11 the public authorities have turned to the private authorities to design the architecture of the systems, to make 'efficient' systems."[12] The concern is that the authorization of groups such as the *Smart Border Alliance* to act to govern the movement of people has, in effect, depoliticized the US VISIT system and normalized its practices on the grounds of expertise and technical know-how.

The extension of border control authority into the private sphere does not end with private firms, however. As Accenture's Eric Stange explained in an interview following the award of the US VISIT contract, what is needed in the war on terror is a "cultural change," a shift that extends beyond governments and firms, and into individuals' perceptions of their own responsibilities (CIO Insight, 2004). Perhaps an example of such a shift towards a state of constant vigilance can be found in Town Compass LLC, a Seattle data company, marketing personal products to fight the war on terror. Their 'Most Wanted Terrorists' database is available as a free download to pocket PCs and smartphones as part of their 'Terrorism Survival' bundle. As Town Compass explain: "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 Military and Aerospace

Electronics, 2004: 4). Should the vigilant citizen succeed in identifying a suspicious person, the package comes complete with one-touch dialling to the FBI and full details of currently available rewards.

The growth of technologies of self-governance has had an important role to play in the extension of risk management in the war on terror. At the time of writing the exit technologies for US VISIT are undergoing pilot trials at selected US airports. Ultimately, however, it will be the responsibility of travellers to "check-out" by scanning their passport and their fingerprints at individual kiosks in departure lounges. Airline passengers are warned during in-flight videos that their exit details are required in order to enable future entry into the United States. In a similar manner to the technologies that establish credit ratings for individuals, the US VISIT system will, over time, have risk "entry and exit" ratings for individuals. Amsterdam's Schiphol airport is already demonstrating future possibilities with its members only 'Privium' programme. Open only to EU-passport holders, $ 145 annual fee and a biometric submission entitles members to expedited security queues and linked frequent flier benefits (Fox, 2004). Such programmes have the effect of inculcating a culture of 'responsible risk taking' where the frequent flier voluntarily engages in the governance of him/herself as well as that of others.

Conclusions

The central issue in the politics of the risk society, according to Beck (2002: 41) is "*how to feign control over the uncontrollable*" (original emphasis). It is possible to argue that targeted governance in the war on terror is one way in which control over the uncertainties of globalization is feigned. As illustrated by Secretary Ridge:

> It's truly no coincidence that the threat to the stability and the peace of the world has coincided with the globalization of technology, commerce, transportation and communication. The same benefits enjoyed by peace-loving, freedom-loving people across the world are available not to terrorists, as well. (Department of Homeland Security, 2004b: 2).

Risk management via targeted governance, then, rests upon the representation of two worlds of globalization: one populated by legitimate and civilized groups whose normalised patterns of financial, tourist and business behaviour are to be secured; and another populated by illegitimate and uncivilized persons whose suspicious patterns of behaviour are to be targeted and apprehended. In order that the legitimate world of profitable global financial

transactions and business and leisure travel can remain an alluring and enduring prospect, control over the illicit world of terrorism, trafficking or illegal immigration must be given credence. As we have argued, the impression of policing the behaviour in the 'illegitimate' sphere rests upon the categorization and risk pooling of normality and suspicion, as well as problematic dichotomies between civil and uncivil everyday practices (Amoore and Langley, 2004: 108–110).

Yet, as Coutin et al. argue (2002: 803), and as we have illustrated, the legitimate and illegitimate spaces of globalization are more "mutually constituting and interdependent" than is normally assumed. In the field of money laundering and terrorist finance, there is increasing evidence that the 'upper worlds' and 'underworlds' are more closely linked and difficult to separate than is assumed in much policy literature (van Duyne et al., 2002). Similarly, the governmental practices of border control do not simply defend the 'inside' from the threats 'outside,' but continually produce our sense of the insiders and outsiders in the global political economy. We have sought here to problematize the techniques and technologies deployed to isolate and segregate the underworld of outsiders from the upperworld of insiders. In a system where verification by dataveillance becomes a condition of being, it is precisely the most subordinate and marginalized groups who will find their identities most difficult to authenticate. From downtown banking halls to city airport terminals, the techniques of dataveillance will continually inscribe and reinscribe a manufactured border between the licit and illicit worlds.

Neglecting the mutuality and contingency of the legitimate/illegitimate worlds of the movement of money and peoples, however, not only serves to further marginalize the poor but also seriously underplays the extent to which risk is deployed as a means of governing contemporary society. Of course, it suits the various players in the homeland security market to talk up the threats and risks of the covert world. As the US business press note, "terror may be your portfolio's security" (Business Week Online, 2004: 14). But, our purpose here has been to challenge the discourse of risk multiplication and intensification that has played such a central role in both the war on terror and the booming homeland security market. From our perspective, and following a tradition of critical thought on risk, it is not so much that new risks have come into being, but that society has come to understand itself and its problems in terms of risk management (De Goede, 2004; Amoore, 2004; Ewald, 1990). Among the implications of this risk-based means of governing in the war on terror, as we have shown, is the ongoing displacement and reallocation of risk that cannot be so easily calculated and controlled.

Notes

1. Though we focus explicitly on the deployment of risk profiling in the governing of the movement of money and people, similar processes of classification and social sorting are at work in the movement of commodities. See, for example, Josiah Heyman's study of the marking out of 'legitimate' commodities at US–Mexico ports of entry (2001), and Brenda Chalfin's work on surveillance by customs agencies at Ghanaian ports (2004). Indeed, the surveillance of commodities at key sites such as airports is tightly interwoven with the classification of legitimate from illegitimate mobilities (Adey, 2004).
2. With the term the 'War on Terrorist Finance' is meant all policy measures and regulatory guidelines issued by governments, private bodies and international institutions designed to detect and prevent the financing of terrorism. The war on terrorist finance is an important component of the war on terror, and some of the most important and far-reaching provisions of the Patriot Act are in the field of financial regulation and prosecution for money-laundering.
3. The debate about the logic and effectiveness of follow-the-money methods in crime policy is ongoing, see for example, Levi (2002, 2003), Naylor (1999), and Nelen (2004).
4. 'Stopping Terrorism Starts with Stopping the Money' poster, to be downloaded at: http://www.ustreas.gov/rewards/.
5. Find the leaflet online at the British Banking Organisation's website: http://www.bba.org.uk/pdf/awareness2.pdf.
6. For the Eight Special Recommendations, see: http://www.fatf-gafi.org/TerFinance_en.htm.
7. Recommendation 25, Forty Recommendations, FATF I, http://www.fatf-gafi.org/pdf/40Rec-1990_en.pdf.
8. Full text of the testimony is available at www.house.gov/reform/tapps/hearings.htm.
9. United States Visitor and Immigrant Status Indicator Technology.
10. Full text of the letter is available at www.epic.org/privacy/us-visit/redress_letter.pdf.
11. Interview with representative of Electronic Privacy Information Center, Washington, DC, November 9, 2004.
12. Interview with civil liberties organization, New York, November 7, 2004.

References

Accenture digital forum, "US DHS to Develop and Implement US VISIT Program at Air, Land and Sea Ports of Entry," 2004, available at www.digitalforum.accenture.com.

Accenture press release, "Government Security Contract to Help Make US Safer," 2004, available at www.carers3.accenture.com/careers/global.aboutaccenture/careersnews/cn-usvisit.

Adey, P., "Secured and Sorted Mobilities: Examples from the Airport," *Surveillance and Society*, 2004 (1: 4), 500–519.

Al-Suhaimi, J., "Demystifying Hawala Business," *The Banker*, 2002, 152(914), 76–78.

Amoore, L., "Risk, Reward and Discipline at Work," *Economy and Society*, 2004 (33: 2), 174–196.

Amoore, L. and P. Langley, "Ambiguities of Global Civil Society," *Review of International Studies*, 2004 (30: 1), 89–110.

Andreas, P. and T. Snyder, (eds.) *The Wall Around the West: State Borders and Immigration Controls in North America and Europe* (Lanham: Rowman & Littlefield, 2000).

Appadurai, A., "Spectral Housing and Urban Cleansing: Notes on Millennium Mumbai," *Public Culture*, 2000 (12: 3), 627–651.

Aufhauser, D.D., "Terrorist Financing: Foxes Run to Ground," *Journal of Money Laundering Control,* 2003 (6: 4), 301–305.

Baker, T., "Liability and insurance after September 11: Embracing Risk meets the Precautionary Principle", *University of Connecticut School of Law Working Paper Series*, 2002.

Beeson, A., "On the Home Front: A Lawyer's Struggle to Defend Rights After 9/11", in R. Leone and G. Anrig (eds.), *The War on Our Freedoms* (New York: Public Affairs/Century Foundation, 2003).

Beck, U., "The Terrorist Threat: World Risk Society Revisited," *Theory, Culture & Society*, 2002 (19: 4), 39–55.

Bester, H., L. de Koker and R. Hawthorne, "Access to Financial Services in South Africa," *Genesis Analytics*, April, 2004, available at http://www.finmarktrust.org.za/documents/2004/April/FATFCaseStudy_2004.pdf.

Bigo, D., "Security and Immigration: Toward a Critique of the Governmentality of Unease," *Alternatives*, 2002 (27), 63–92.

Brisbin, R., "Old Standards and New Practices of Governing: Federalism and Rights Paradigms and the Risk-Management Regime", paper presented at the annual convention of the American Political Science Association, 2004, 2–5 September, 2004.

Business Week, "The Price of Protecting the Airways," 2001, available at www.businessweek.com/print/technology/content/dec2001/tc2001124_0865.htm.

Business Week, "Welcome to Security Nation," 2004a, 3887, p. 32.

Business Week, "Accenture Hits the Daily Double," 2004b, 3891, p. 74.

Business Week Online, "Terror May be Your Portfolio's Security," 16 August, 2004, www.buinsessweek.com/print/bwdaily/dnflash/aug2004/nf20040816_9987_db014.htm?chan=d,

Campbell, D., "With Pot and Porn Stripping Corn, America's Black Economy is Flying High," *The Guardian*, 2 May, 2003, p. 3.

Campbell, D., "Introducing Del-Qaida," *The Guardian*, 17 July, 2004, p. 17.

CIO Insight, "Beta," August, 2004, 42, p. 22.

Chalfin, B., "Border Scans: Sovereignty, Surveillance and the Customs Service in Ghana," *Identities: Global Studies in Culture and Power*, 2004 (11), 397–416.

Clarke, R., "Dataveillance: Delivering 1984," in L. Green and R. Guinery (eds.), *Framing Technology: Society, Choice and Change* (London: Routledge, 1994).

Coutin, S.B., *Legalizing Moves: Salvadoran Immigrants' Struggle for US Residency* (Ann Arbor: University of Michigan Press, 2000).

Coutin, S.B., B. Maurer and B. Yngvesson, "In the Mirror: The Legitimation Work of Globalization," *Law and Social Inquiry*, 2002 (27: 4), 801–843.

De Genova, N.P., "Migrant Illegality and Deportability in Everyday Life," *Annual Review of Anthropology*, 2002 (31), 419–447.

De Goede, M., "Repoliticising Financial Risk," *Economy and Society*, 2004 (33: 2), 197–217.

De Goede, M., *Virtue, Fortune and Faith: A Genealogy of Finance* (Minneapolis: University of Minnesota Press, 2005).

Department of Homeland Security, "DHs Announces Award of US VISIT Prime Contract to Accenture LLP," 2004a, available at www.dhs.gov/dhspublic/display?theme=43&content.

Department of Homeland Security, "Transcript of Secretary of Homeland Security Tom Ridge at the Center for Transatlantic Relations at Johns Hopkins University," 2004b, available at www.dhs.gov/dhspublic/display?theme=44&content=3994&print=true.

Department of Homeland Security, "Remarks by Secretary of Homeland Security Tom Ridge at the European Policy Centre," 2005, available at http:www.dhs.gov/dhspublic/display?content=4293.

Doty, R.L., *Anti-Immigrantism in Western Democracies: Statecraft, Desire and the Politics of Exclusion* (London: Routledge, 2003).

Ewald, F., "Norms, Discipline and the Law," in R. Post (ed.), *Law and the Order of Culture* (Berkeley: University of California Press, 1990).

Forbes.com "Biometrics Beyond Terrorism," 2004 available at http://www.forbes.com/2004/07/08/cx_pp_0708biometrics_ii_print.html.

Fox, P., "The Security Privilege," *Computerworld*, 2004 (38: 23), 1.

Fox, W.J., *Speech Before the Anti-Money Laundering Compliance Conference* (New York: Securities Industry Association, 2004a), 4 March, available at http://www.fincen.gov/foxsia030404.pdf.

Fox, W.J., *Statement Before the United States House of Representatives*, Committee on Financial Services, 16 June, 2004b, available at http://www.fincen.gov/hfscommitteestatement061604.pdf.

FSA, Financial Services Authority, *Reducing Money Laundering Risk: Know Your Customer and Anti-Money Laundering Monitoring*, 2003, Discussion Paper 22, August, available at http://www.fsa.gov.uk/pubs/discussion/dp22.pdf.

Gillespie, J., *Follow the Money: Tracing Terrorist Assets*, Seminar on International Finance, Harvard Law School, 15 April, 2002, available at http://www.law.harvard.edu/programs/PIFS/pdfs/james_gillespie.pdf.

Heimer, C., "Insuring More, Ensuring Less: Private Regulation Through Insurance," in T. Baker and J. Simon (eds.), *Embracing Risk: The Changing Culture of Insurance and Responsibility* (Chicago: University of Chicago Press, 2002).

Heyman, J., "Class and Classification on the US-Mexican Border," *Human Organization*, 2001 (60), 128–140.

Horst, C. and N. van Hear, "Counting the Cost: Refugees, Remittances and the 'War against Terrorism,"' *Forced Migration Review*, 2002 (14), 32–34.

Kestelyn, J., "For Want of a Nail," *Intelligent Enterprise*, 2002 (5: 7), 8.

Langley, P., *The Everyday Life of Global Finance*, IPEG working paper, British International Studies Association, 2002, available at http://www.bisa.ac.uk/groups/ipeg/papers/PaulLangley.pdf.

Larner, W. and W. Walters, "Introduction: Global Governmentality: Governing International Spaces," in W. Larner and W. Walters (eds.), *Global Governmentality: Governing International Spaces* (London: Routledge, 2004).

Levene, T., "Why Rules Won't Wash on Money Laundering," *The Guardian Jobs and Money*, 2003, 28 June, 2–3.

Levi, M., "Money Laundering and Its Regulation," *Annals of the AAPSS* 2002 (582), 181–194.

Levi, M., "Following the Criminal and Terrorist Money Trails," in P. C. van Duyne, K. von Lampe and J.L. Newell (eds.), *Criminal Finances and Organising Crime in Europe* (Nijmegen: Wolf Legal Publishers, 2003).

Levi, M. and D.S. Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society," *Journal of Law and Society*, 2004 (31: 2), 194–220.

Leyshon, A. and N. Thrift, "Lists Come Alive: Electronic Systems of Knowledge and the Rise of Credit-Scoring in Retail Banking," *Economy and Society*, 1999 (28: 3), 434–466.

Lyon, D., *Surveillance Society: Monitoring Everyday Life* (New York: Routledge, 2001).

Lyon, D., *Surveillance After September 11* (London: Polity, 2003a).

Lyon, D., (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (New York: Routledge, 2003b).

Lyon, D., "Identity Cards: Social Sorting by Database," *OII Issue Brief* 2004, no. 3.

Maimbo, S.M., *The Money Exchange Dealers of Kabul*, Worldbank Working Paper, June, 2003, no. 13.

Malkin, L. and Y. Elizur, "The Dilemma of Dirty Money," *World Policy Journal*, 2001, (Spring), 13–23.

Malkin, L. and Y. Elizur, "Terrorism's Money Trail," *World Policy Journal* 2002 (Spring), 60–70.

Mantas, "Money Laundering – Keep it Clean," *Banking Technology*, 30 November, 2003, available at http://www.mantas.com/NewsEvents/News/BankingTechnology113003.html.

Military and Aerospace Electronics, "Homeland Security Focus," 2004 (15: 7), 4.

Naylor, R.T., "Wash-Out: A Critique of Follow-the-Money Methods in Crime Control Policy," *Crime, Law & Social Change*, 1999 (32), 1–57.

Nelen, H., "Hit Them Where It Hurst Most?," *Crime, Law and Social Change*, 2004 (41), 517–534.

O'Harrow, R., *No Place to Hide* (New York: Free Press, 2005).

O'Malley, P., "Uncertain Subjects: Risks, Liberalism and Contract," *Economy and Society*, 2000 (29: 4), 460–484.

Passas, N., *Informal Value Transfer Systems and Criminal Organisations: A Study into So-Called Underground Banking Networks*, Dutch Ministry of Justice, 1999, available at http://www.minjust.nl:8080/b_organ/wodc/publications/ivts.pdf.

Passas, N., "Law Enforcement Challenges in Hawala-Related Investigations," *Journal of Financial Crime*, 2004a (12: 2), 112–119.

Passas, N., "Indicators of Hawala Operations and Criminal Abuse," *Journal of Money Laundering Control*, 2004b (8: 2), 168–172.

Peterson, V.S., *A Critical Rewriting of Global Political Economy* (London: Routledge, 2003).

Pieth, M., "Financing of Terrorism: Following the Money," *European Journal of Law Reform*, 2002 (4: 2), 365–376.

Rose, N. and V. Mariana, "Governed by Law?," *Social and Legal Studies*, 1998 (7: 4), 541–551.

Roth, J., D. Greenberg and S. Wille, National Commission on Terrorist Attack upon the United States, *Monograph on Terrorist Financing*, 2003, available at http://www.9–11commission.gov/staff_statements/911_TerrFin_Monograph.pdf

Sassen, S., *The Global City: London, New York, Tokyo* (Princeton, NJ: Princeton University Press, 1991).

Stein, N., "The Fruits of Safety," *Fortune (Europe)*, 2004 (149: 11), 11.

Theil, S., "Gordon Woo: Calculus for Catastrophe," *Newsweek*, 12 July, 2004, available at http://www.msnbc.msn.com/id/5352360/site/newsweek/

Thrift, N., "Movement-Space: The Changing Domain of Thinking Resulting from the Development of new Kinds of Spatial Awareness," *Economy and Society*, 2004 (33: 4), 582.

US Department of the Treasury, *A report to Congress in Accordance with Section 359 of the USA Patriot Act*, November, 2002, availale at http://www.fincen.gov/hawalarptfinal11222002.pdf.

US Department of the Treasury, *National Money Laundering Strategy 2003*, 2003, available at http://www.ustreas.gov/offices/eotffc/publications/ml2003.pdf.

Valverde, M. and M. Mopas, "Insecurity and the Dream of Targeted Governance," in W. Larner and W. Walters (eds.), *Global Governmentality: Governing International Spaces* (London: Routledge, 2004).

van der Ploeg, I., "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, 2003).

van Duyne, P.C., K. von Lampe and N. Passas, *Upperworld and Underworld in Cross-Border Crime* (Nijmegen: Wolf Legal Publishers, 2002).

Walters, W., "Mapping Schengenland: Denaturalizing the Border," *Environment and Planning D*: *Society and Space*, 2002 (20), 561–580.