Transactions after 9/11: the banal face of the preemptive strike

Amoore, L.; de Goede, M.

Published in:
Transactions - Institute of British Geographers

DOI:
10.1111/j.1475-5661.2008.00291.x

Transactions after 9/11: the banal face of the preemptive strike

Louise Amoore* and Marieke de Goede**

This paper argues that the deployment of transactions data of many kinds has become the banal face of the war on terror's preemptive strike. Because the failure to predict and prevent 9/11 is partly thought to be a failure to 'connect the dots' of available intelligence, post 9/11 policies seek to register, mine and connect ever more 'dots', or association rules, in the form of credit card transactions, travel data, supermarket purchases and so on. We argue that it is in these ordinary transactions that another spatiality of exception is emerging, one in which the traces of habits, behaviours and past practices become the basis of security decisions to freeze assets, to apprehend, to stop and search or to deport. As such, these developments constitute a relatively unacknowledged violence in the war on terror, which is in need of critical questioning.

key words war on terror transactions surveillance pre-emption political geography privacy

*Department of Geography, University of Durham, Durham DH1 3LE
email: louise.amoore@durham.ac.uk
**Department of European Studies, University of Amsterdam, 1012VB Amsterdam, The Netherlands

revised manuscript received 25 October 2007

> If we learned anything from September 11 2001, it is that we need to be better at connecting the dots of terrorist-related information. After September 11, we used credit card and telephone records to identify those linked with the hijackers. But wouldn't it be better to identify such connections before a hijacker boards a plane? (Chertoff 2006, A15)

> The exception becomes the norm, every transaction becomes like a credit card. (Kang 1998, 106)

Introduction: 'Keep the data flowing and the planes flying'

During the summer of 2006, two apparently unremarkable events revealed a glimpse of the, otherwise concealed, everyday security practices of the war on terror. In June, it was revealed that the Brussels-based financial clearing house SWIFT had routinely extradited banking and credit card transactions data to the US security services. The geographies of a global war on terror, it seemed, drew the mundane financial transactions data of European and North American citizens into cross-border extradition in the name of homeland security. Only one month earlier, the European Court of Justice had ruled that the EU–US agreement on the sharing of airline passenger data be annulled on the grounds that it breached rights to privacy (Guild and Brouwer 2006). The Passenger Name Record (PNR) agreement of 2004 required that airlines submit 34 items of data on each passenger – including, for example, credit card numbers, previous travel activity and in-flight meal choices – within 15 minutes of flight departure for the US. In both instances, the transaction is represented as a means of reconciling mobility with security or, as for the Department of Homeland Security, a way to 'keep the data flowing and the planes flying' (DHS 2006).

How, then, has the extradition of data on transactions of many kinds become the condition of security for post 9/11 geopolitics? In this article, we argue that the transaction is becoming central to security practice because it is assumed to provide a complete picture of a person, an 'electronic footprint' that makes it possible to identify a suspicious body in movement and, most importantly, to verify or deny access *in advance*. Though we are profoundly

ISSN 0020-2754

interested in the changing practices of surveillance after 9/11, and have considered their political implications elsewhere (see also Amoore and de Goede 2005; Lyon 2003; Lyon and Bennett 2008), it is not surveillance per se, but rather the specific question of security authorisation *in advance* that concerns us in this article. As Greg Elmer and Andy Opel put the question of the difference between surveillance and preemption:

> In an environment of already made, or pre-made decisions ... we believe there is a need to rethink theories of social control that have evolved out of the pervasive use of surveillance. (2006, 479)

Here, we invoke Michel Foucault's crucial distinction between the essentially *disciplinary* procedures of *surveillance* and the contemporary apparatus of *security*. In his 1978 lectures at the Collège de France, Foucault depicts the panopticon as 'completely archaic', and 'the oldest dream of the oldest sovereign' (2007, 66). In contrast to the 'exhaustive surveillance of individuals', a 'discipline' that 'concentrates, focuses and encloses', Foucault observes an 'apparatus of security' that 'opens up' to 'let things happen' (2007, 44–5). Put simply, where disciplinary surveillance predicts, surveys and prohibits, the apparatus of security preempts, visualises and opens to circulation (cf. Agamben 2002; Massumi 2007; Crandall 2007). As in our opening citation, the contemporary security apparatus renders the transaction a means of identifying and apprehending a potential perpetrator before a plane is boarded, a bank account is accessed, a subway station is entered or a border is crossed. In short, we argue that the transaction is not primarily a disciplinary mechanism of surveillance, but instead has become a specific preemptive means of securing in the face of an uncertain future. It is in this sense, we argue, that transactions can be understood as the banal face of the preemptive strike.

In the aftermath of 9/11, the Madrid and London bombings, political authorities in the West have pursued the idea that knowledge about future risk is *always already present* in the data, if only information on transactions patterns can be effectively integrated and mined. Indeed, in 2003 a US joint inquiry concluded that 'on September 11, enough relevant data was resident in existing databases' so that 'had the dots been connected, the events could have been exposed and stopped' (US Joint Inquiry 2003, 14). In this way, the sovereign lines that designate the exceptional spaces of the war on terror are not limited to the oft-cited Abu Ghraib, Guantanamo Bay and extraordinary rendition flights (Agamben 2005; Butler 2004; Edkins *et al.* 2004). In our view, though these are intolerable examples of the logic of the camp that deservedly attract attention, there are other violences at work in the war on terror that are relatively unacknowledged and, perhaps as a result, are in danger of being accepted as ubiquitous features of contemporary life. They are the more prosaic prejudices concealed in the actions taken on the basis of the minutiae of daily life – the newspaper bought at a railway station, the wire transfer made from an Amsterdam branch of Western Union, the cash paid for an airline ticket. Indeed, it is precisely on the basis of such transactions that people are stopped at the border, separated from their families and enter the circuits of extraordinary rendition and offshore detention.[1] As Michael Shapiro (2007, 301), drawing on the work of A.R. Stone, has argued, the new 'violent cartography' of the war on terror entails the spatialisation of the 'legible bodies', 'whose textually mediated physicality extends to its paper and electronic trail'. Thus, we argue, in the ordinary transactions of daily life another spatiality of exception is emerging. Not only are all transactions made to acquire the traceability of a credit card, as in Jerry Kang's sense of the exceptional payment system becoming the norm, but transactions become precisely the basis for designation of exception, for the settling out of finite differentials of normality and deviation.

It is important to emphasise here that we are not arguing that the use of transactions data after 9/11 is unique or unprecedented – there is ample historical evidence of risk profiling via data prior to 9/11 (Haggerty and Ericson 2000; Andreas and Snyder 2000; Thrift and French 2002; Graham 2005). However, the specific representation of threat and danger *after 9/11* – terrorists who 'live among us'; 'home grown terrorists'; 'clean skins' and so on – has cleared the ground for the deployment of commercial data as a basis for (preemptive) security action. Although the risk practices involved in transactions data mining are far from new (we need only look to the history of insurance or credit scoring, for example), the scale and scope of their application to the sphere of security is distinctly novel, and entails practices of actionable visualisation that depart significantly from established uses of surveillance technologies in urban policing.

In this paper, we offer substantive detail on the deployment of commercial transactions data in the

Trans Inst Br Geogr NS 33 173–185 2008
ISSN 0020-2754

security domain to govern the mobility of people and the mobility of money. These two spheres that are often analysed in separation are closely intertwined in practice, with financial transactions increasingly used as a means of profiling travellers, and corporeal identification and locatability required for access to the financial system. As the example of the Oyster Card analysed below demonstrates, 'access points' of travel data in border control and urban policing are often thoroughly integrated with new payment options. In turn, financial data, such as credit card transactions and wire transfer data are now thought to be among the most reliable sources for determining whether a traveller requires a 'closer look' at the border. In this sense, then, it is not possible to distinguish new ways of governing money from new ways of governing people, and this paper is interested precisely in the question of how financial and travel data work in conjunction to produce new spaces of governing in the war on terror. Though we are concerned to situate our discussion in these two specific domains, moreover, we are motivated by a set of questions and concerns that exceeds them. In the first section we ask, if transactions of many kinds are to be understood as having geopolitical significance, what kind of space of governing is emerging? As transactions data oscillate back and forth between commercial and security applications, do they form a 'complex assemblage' with a novel spatiality of its own (Connolly 2004, 35)? In the second section we consider the temporality of the security decisions that are made on the back of transactions data. How are decisions about risk and norm authorised? How does knowledge about *past* incidents, habits and so on, drawn from patterns of transactions, become the *present* profile of a body 'at risk' or 'risky' in the *future*? Finally, we conclude with a discussion of some of the political implications of techniques that classify via the transaction. Do the practices enacted via the transaction constitute a form of political violence that is more often concealed within the broader rubric of the war on terror? In what ways might they be politicised, opened up to broader societal engagement?

Transactions/space

Moving quickly through the crowds of the ticket hall at a London Underground station, a young woman stops to top up her Oyster payment card at a nearby machine. The transaction cannot be authorised, the machine tells her, she must report to the officials in the booth. From behind the glass, the Transport for London worker taps at the computer keyboard:

> 'Yes, I can see the problem, you did not complete your journey on September 29th'.
>
> 'But I must have . . . I am here now'.
>
> 'No, we have no exit record of your smart card, your journey is incomplete. If you can just tell me where you completed your journey that day, I can reactivate your card'.
>
> 'But, I don't remember, it is two weeks ago'.
>
> 'I can tell you that you began your journey at Russell Square at 15.20 pm . . . we just need the exit data to complete the transaction'.[2]

In the travel transactions data of the payment card, the mobile people of the city leave their mapped traces. The completion of a journey and the registration of the travel card to a verifiable address – like the timely repayment of a loan, or a pattern of no-claims on motor insurance – identifies and marks out the low-risk traveller, allowing her to be targeted, for coupons and discounted travel, or for intervention and interception. In effect, when established patterns are breached, the woman is asked to repair her risk rating, to complete her transaction and leave verifiable data.

In what has become the calculative and ever-vigilant face of the war on terror, the transaction has become the primary means of reconciling the mobility and security of public space. Indeed, the etymology of *transaction*, with its root in *trans* (through) and *agere* (to drive), and in the Latin *transactio* (an agreement), speaks to the authorisation of a crossing or passing through. As we have seen affixed to the walls of all US land, air and sea ports of entry under the USVISIT system, for example, data on our transactions has become an important means of 'keeping America's doors open and our nation secure'.[3] Transactions data, then, are imagined as means of *both* freeing up mobile people in global cities, at airports or land border crossings, and securing and verifying their identity and credibility. Understood in this way, transactions become a specific means of governing life, a biopolitical move that governs by acting on and through life itself (cf. Dean 1999). In contrast to a sovereign power that stands at the centre of 'disciplinary space', 'establishing limits and frontiers, or fixing locations',

ISSN 0020-2754

then, the apparatus of security involves 'making possible, guaranteeing, and ensuring circulations' (Foucault 2007, 29; also Elden 2007). Because the transactions people make are, quite literally, taken to be the traces of daily life, they are conceived as a way of mapping, visualising and recognising bodies in movement. In this sense the novel borderings of the war on terror are distinctive precisely because they permit the mobile drawing of lines: the physical jurisdictional border seeps into data and databases, and into the urban architectures of our lives. In the post 9/11 context, transactions data have acquired a seductive allure because they appear to make it possible to continue to permit mobility, even to enhance or accelerate movement for some, whilst using those patterns of mobility as the basis for security decisions that enact the border in new ways.

Though political authorities have historically engaged routine surveillant *data collection* and *categorisation* in, for example, the governance of immigration and border security (Walters 2002), what we are seeing now is a move to *data mining* that classifies mobile people and objects into degrees of risk. There is an important distinction to be made here. In contrast to the survey, the audit, the records of data collection, we find in data mining a system of risk governing, described by Foucault as 'exactly the opposite of the one we have seen with discipline' (2007, 63). The identification of risk – differential dangers, risky bodies, risk zones, risk scores – draws private commercial techniques and expertise into state security in novel forms that are not primarily surveillant (Amoore and de Goede 2008). In short, it is not the collection, monitoring or 'sight' of data that is significant, so much as the way decisions are made on the basis of a risk analysis that 'foresees'.

Data mining techniques have become ubiquitous commercial methods for identifying patterns and relationships in large volumes of data, enabling the analysis of behaviour, anomaly detection and targeted risk analysis. With its origins in an experimental relationship between IBM Research Fellow Rakesh Agrawal and UK retailer Marks & Spencer in the early 1990s, transactions data mining promised to identify 'association rules' between specific items in a large data set (Agrawal *et al.* 1993). In the retail context, this could be something as simple as the association between purchases such as milk and bread, using the data to tailor vouchers and coupons at particular customer profiles. Now that Agrawal and his colleagues are directing these same techniques at security – leading what they call 'the mathematical sciences role in homeland security' (BMSA 2004) – transactions data are deployed to look for association rules between other kinds of patterns of life. The purchase of an airline ticket, patterns of past travel, credit card use – all can be potentially transformed by association rules into degrees of risk. As former Attorney General, Michael Chertoff, has explained it:

> Through what has come to be called 'data mining' and predictive technology, we seek to identify potential terrorists. In a search for terrorists and terrorist cells, we are employing technology that was previously utilized primarily by the business community. (US Department of Justice 2002)

Thus, for example, the integration of databases containing airline passenger information, visa applications, asylum seeker and refugee status, biometric identifiers and so on becomes a tool that makes disparate data searchable and actionable for security decisions. In the US context, the USVISIT system has deployed data in this way since 2004, integrating databases as diverse as student visas, vehicle licences and credit card records in order to derive association rules (Amoore 2006; Sparke 2006).

Financial transactions data are regarded as particularly important in the context of visualising terrorist networks and enabling security action. This is not so much because, as the US Treasury has it, 'stopping terrorism starts with stopping the money'.[4] More importantly, financial transactions data are considered valuable because it is assumed that 'money trails don't lie' (Snow 2006) and financial data are thought to have the ability to disclose 'blueprints to terrorist organisations' (Zarate 2004). As one US Treasury insider puts it, financial data mining was accorded a central role within the war on terror because of its preemptive promise: financial data are regarded as

> extremely useful in tracing and investigating mere suspicions so that you might also similarly prevent a calamity that *you don't yet have definition on.* (Council on Foreign Relations 2007; emphasis added)

The deployment of financial data in the war on terror does not just draw credit card and wire transfer data into security practice, but also redeploys commercial risk techniques pioneered in financial markets in novel ways (Martin 2004). Perhaps the most prominent and controversial

ISSN 0020-2754

instance when financial transactions data held by a commercial institution were seized and mined in the context of terrorist investigations was when the US Treasury subpoenaed millions of records from Belgian-based banking cooperative Society for Worldwide Interbank Financial Telecommunication (SWIFT). These records were deployed precisely for the investigation of 'mere suspicion' to enable preemptive security action: searches by names of blacklisted persons and potential suspects were used in order to determine their associates and *their* associates. In this way, the 'association rules' governing the mathematical logics of data mining become the juridical equivalent of guilt *by association*.[5]

To clarify our point here, it is not simply that transactions data are redeployed to secure particular spaces, but that – because the data are approached and analysed through risk-based calculative models that aim to identify suspicious populations and unusual activity – they are producing new spaces of governing, and the exceptions and exemptions that apply to those spaces. In particular, the deployment of transactions data might be seen as a novel risk technology because it targets that which is 'outside' – the 'anomalous' transaction, the 'suspicious' body, the deviant pattern of behaviour – precisely in order to reincorporate it within governable space. In this sense, transactions data could be interpreted as one means by which the contemporary state declares the exception, what Giorgio Agamben calls a 'technique of government' that 'takes outside' in order to include within the juridical order (1995, 9; 2005, 26). Yet, some caution is needed here if we are to grasp what is truly significant about the new spaces of governing we see emerging. The 'violent geographies' that many have depicted in places such as Guantanamo Bay and Abu Ghraib, and in the presence of military personnel on our city streets, are rather more subtly drawn in the prosaic geographies of daily transactions (Gregory and Pred 2007; Katz 2007). The process of 'taking outside' via the identification of transactions that are deviant 'others' remains little understood.

Consider, by way of example, the announcement in December 2006 that London's Oyster travel payment system is to link up with Barclaycard and Visa Europe. The new 'wave and pay' technology will enable commuters to use their Oyster-Visa card to pay, quite literally 'on the move', for small items (newspapers, bottled water, postage stamps and so on) that previously would have been integral to the cash economy. The contactless radio frequency chip already present inside Oyster travel cards means that mobile bodies and mobile transactions will become increasingly intertwined, as people make transactions 'in transit' without directly scanning their cards. As the Mayor of London, Ken Livingstone, announced at the Transys launch, Oyster has 'made journeys across London cheaper, easier, quicker' and, in the future 'people can buy low cost items on the same card, reducing the need to carry cash' (Transport for London 2006). Of course, the Oyster-Visa collaboration draws a wider array of transactions into observable and governable space. By placing risk flags on anomalous or atypical transaction patterns – driving out cash transactions or simply marking them as atypical – the system has the potential to include mobile bodies – 'keep London moving'; 'keep the planes flying'; 'keeping the doors open' – precisely by means of a radio frequency 'tagged' exclusion that keeps open the possibility of intervention, detention, interception at any time in the future.

Understood in this way, the use of transactions data as a security device is one means by which borders and boundaries are simultaneously loosened and tightened, re-drawn across the ordinary spaces of city subways, suburban railway stations or sports stadiums.[6] We begin to see the drawing of boundaries that extend from the city streets, across the routines of daily life and into the records and traces of the transactions we leave behind us. 'Identity fences replace territorial fences', writes Didier Bigo, 'while people are allowed to move, their identities must be constructed and controlled' (2002, 115). Transactions data, in this context, are considered key not just because they seem to anchor 'informal and unstructured' terrorist networks (Levitt 2004, 34), but also because they are seen to anchor *identity*. The ambitions of security data mining are to 'build a complete picture' of a person by integrating travel data, financial data, library records driving records etc. (Stanley 2004, 23). It is important to note here that data-integration techniques seek to establish people's identity partly through their apparent social embedding. The question intelligence services ask is: 'Is this individual a known and rooted member of the community?' (Michael Jackson, quoted in Curry 2002, 494). When global management consultants Accenture were bidding for a multi-billion US dollar contract to create 'smart borders', they appealed precisely

ISSN 0020-2754

to this ability to build a complete picture of a person through their social network:

> The old system 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. (*Business Week* 2001, 1)

The deviant other, then, is identified not so much through her individual aberration from a norm, but through an assembly of transactions or associations seen as signifying suspicious activity. Again, in the security apparatus the norm functions quite differently from that in disciplinary procedures of surveillance. 'What is involved in disciplinary techniques is a *normation*', suggests Foucault, 'rather than normalization' (2007, 57). The distinction, in short, is that discipline posits a normal 'model' and tries to 'get people, movements and actions to conform to this model', while security uses risk to allow for 'differential normalities' (63). This matters greatly to the juridical decisions that can be taken on the basis of transactions screening. Where juridical disciplinary mechanisms would draw a clear line of prohibited and permitted transactions, the security apparatus is quite different. In the case of asset freezing, for example, a differential norm may enable the exceptional treatment of a suspect, as former Treasury Secretary Paul O'Neill puts it, 'on the basis of evidence that might not stand up in court' (quoted in Suskind 2004, 192).

This does not mean, of course, that we argue that such technologies exist as all-encompassing and all-seeing mechanisms deployed by the state. On the contrary, we argue that these moves enable complex assemblages of government in which important fusions between public and private entities take place. As such, we understand transactions to be an element of what William Connolly (2005, 144) describes as a 'complex assemblage' fashioned by 'resonances' between multiple sites of authorisation. Such an assemblage includes government officials, security experts, risk analysts and information technology consultants, but also the technological constructs articulated and deployed by these experts, including transactions data, algorithmic risk models, network charts and risk indicators. The agency of assemblages, according to Jane Bennett, is the 'distinctive efficacy of a working whole made up, variously, of somatic, technological, cultural and atmospheric elements' (2005, 447). The process of 'taking outside' via the articulation of the exception, thus, is to be understood as more complex than the handing down of a clear-cut decision by an embodied sovereign – located, or not, in state agency. If the sovereign is *that* which decides the exception, according to Connolly (2005, 145), we must understand *that* to be 'composed of a plurality of forces circulating through and under the positional sovereignty of the official arbitrating body'. In our understanding, such plurality of forces includes both the risk analysts and the models they build, both the security experts and the imagination they deploy, both the mid-level bureaucrat and the law they exceed.

Transactions/time

We have argued that the assemblage and analysis of mundane commercial transactions plays an increasingly important role in security decisions. Knowledge about past incidents, behaviours and habits – derived from transactions data – becomes a form of actionable intelligence. Such security decisions are not primarily understood to concern the apprehension and prosecution of terrorists and criminals after they act, but to enable the *preemption* of what could be terrorist schemes or attacks. As the quote heading this paper puts it, the sovereign ambition is to connect the dots '*before* the hijacker boards the plane'. The logic of preemption with respect to disrupting terrorist networks plays out not just in relation to the much-discussed 'preemptive strike' on Iraq, but also in everyday, mundane ways, in which transactions data – including library records, communications data, financial transactions and travel records – come to play a key role. The screening of transactions data thus becomes the war-on-terror's banal face of the preemptive strike.

In its orientation to the unknown future, then, preemptive transactions screening exceeds the logic of the surveillance of 'transaction-generated capta' (Dodge and Kitchin 2005b, 858), and instead projects data forward, allowing for a whole new line of sight. To be clear, what matters is not strictly access to data, nor even the holding, capture or possession of data, but rather what becomes possible via a freeing up of the circulation of data. 'By working with the reality of fluctuations [. . .] and not by trying to prevent it', Foucault reminds us, 'an apparatus is installed which is an apparatus of security and no longer a juridical-disciplinary

ISSN 0020-2754

system' (2007, 37). Indeed, the current moment across the arts, humanities and social sciences is deeply marked by thought on the consequences of moves beyond survey and prediction, to consider preemptive security. 'Preemption is not prevention', writes Brian Massumi, 'prevention operates in a world in which uncertainty is a function of a lack of information' (2007, 1). In this sense, prevention seeks to capture more and more information precisely in order to 'close off', to 'produce order' and to 'prescribe and prevent events' (Agamben 2002, 2). Preemption, by contrast, acts and decides precisely on the basis of an absence or an unknown, on the basis of that which can never be captured. Thus, preemption acts 'by an opening and a globalisation', not to prevent crisis but to 'guide disorder' (Agamben 2002, 2).

The logic of preemption with respect to transactions data, then, is increasingly seen to have to deploy *imagination* in order to profile that which has not yet occurred. The realm of preemption is one of scenario planning, disaster rehearsal, stress testing and Hollywood imagination (Salter 2008). This is where security decisionmaking is enabled, 'not in a context of certainty, nor even of available knowledge, but of doubt, premonition, foreboding, mistrust, fear and anxiety' (Ewald 2002, 294).[7] The decision taken preemptively is one that 'fuels suspicion' and 'invites one to take the most far-fetched forecasts seriously' (Ericson 2007, 23). Similarly, in Richard Grusin's analysis of 'premediation': 'Unlike prediction, premediation is not chiefly about getting the future right'; rather, it is about 'trying to imagine or map out as many possible futures as could possibly be imagined' (2004, 28). For example, one member of the Bush administration recounts how, in the days and weeks after 9/11, White House 'Situation Room' meetings were dedicated to imagining the worst: 'What about poison in the New York reservoir system? What about a private plane flying into a nuclear reactor?' (Taylor 2007, 5).

To summarise our argument to this point, rather than confronting the uncertainty of the future in all its political difficulty and contingency, preemption makes uncertainty a basis for *action*. Security interventions in the mobility of money and the mobility of people are now actively pursued, even if the level and nature of specific threats remains uncertain. Transactions data, we argue, have become key bases of such everyday interventions – whether this is to stop and search on the subway, to intercept a wire transfer, to close a bank account. Such deployment of transactions data is markedly different from established logics of surveillance, in that it is oriented toward enabling preemptive intervention, rather than the creation of a 'machine readable world' (Dodge and Kitchin 2005b, 870). Thus, transactions data, held by commercial players already attuned to imagining the future desires and affective worlds of their consumers, become a means of anticipating future security threats (Ewald 1994; Crandall 2005).

Thus, transactions data become one element of a broader assemblage of 'screening' practices that algorithmically designate and classify the population (Amoore 2007). The temporality of this assemblage is one of folded futures, where there is explicit deployment of imagination, affective perceptions, speculation and media grammars. As Brian Massumi has argued,

> rather than acting in the present to avoid an occurrence in the future, pre-emption brings the future into the present. It makes present the future consequences of an eventuality that may or may not occur, indifferent to its actual occurrence. (2005, 7–8)

The temporality of the transaction thus becomes anticipatory – a means of acting immediately in the face of an uncertain future. Thus, as Massumi suggests, it would scarcely matter if the risk flagged transaction was the purchase of fertiliser, or hydrogen peroxide, or if it was the cash purchase of an airline ticket, or the transfer of small remittance payments. What matters is the imagination of the threat that the future may already hold, such that a preemptive strike is made possible.

What, then, is the role of imagination and preemption in the anticipatory security decision? When, on what basis, by whom, is a decision finally taken? For Massumi, the temporality of the preemptive decision is a 'lightening strike' of sovereign power, where to 'admit to discussing, studying, consulting, analysing' is also to 'admit to having been in a state of indecision' (2005, 5–6). What Massumi overlooks here is the extent to which the contemporary practices of preemption do actually engage in a form of calculation, consulting and analysis, but of a type that effaces the decision itself.

Rather than see the absence of consultation and analysis characterising sovereign decisions, we see precisely the extent of the modern state's engagement with expertise as the eradication of the possibility of decision, and the rendering of decision as perennially deferred. As Jacques Derrida reminds

ISSN 0020-2754

us, 'the decision, if there is to be one, must advance towards a future which is not known, which cannot be anticipated' (1994, 37). A decision that simply algorithmically calculates on the basis of transactions data, then, is not a decision at all, but merely 'the application of a body of knowledge' (37). Of course, security decisions to intervene or intercept are made all of the time (Prozorov 2005), but not all of them eschew mere calculation, not all are responsible in the sense of confronting the political difficulties of indecision. In the dispersed practices of the contemporary security apparatus, we may never know if a decision *is* a decision – made in the context of difficulty, contingency, political uncertainty – or if it has been 'controlled by previous knowledge' and 'programmed' (Derrida 1999, 281). Indeed, as legal scholar Fleur Johns (2005, 631) has argued perceptively, the juridical orders and political designations of exceptionality post-9/11 have largely been framed in terms of 'deferral and disavowal', 'in other words, as non-decisions'.

The move to make transactions data the basis for security decisions is potentially also a move to defer decision into a series of calculations: What is this person's risk profile? Was the journey completed? Does the bank account activity fit the profile of the stated occupation? The tracking and tracing of transactions of many kinds appears to allow for the perennial deferral of decision, for the always possible intervention in the face of imminent surprise or threat.

Transactions/politics

We have argued that the screening of transactions data is the war on terror's banal face of the preemptive strike. While the mundane interventions made on the basis of transactions data have been highlighted in social and spatial analysis (cf. Dodge and Kitchin 2005a 2005b 2006), their implications for geographical and political literatures on security have not been fully acknowledged. Like the direct and visceral military preemptive strike, the deployment of transactions within the security apparatus raises substantial political questions concerning the way in which it governs, selects, identifies and misidentifies its targets. Consider the example of the British Muslim family whose house was raided at dawn in June 2006, after which all family members were arrested and one of them was shot. When, in the weeks after the raid, evidence grew that the suspects were wrongly accused and arrested, the police leaked news that £38 000 in cash was found at the raided property to British tabloid *The Sun*. *The Sun* made this information headline news and wrote:

> The fortune – in *CASH* – was allegedly found in a bedroom after the pair were arrested in a swoop on their modest terraced home ... Last night a security source said: 'It was a hell of a lot to have knocking around. The cash was in a bedroom, much of it in £50 notes. Urgent inquiries are being carried out to trace the source of the money and what it was intended for.' *Police were desperate to learn how Kahar, a postal worker, and Tesco shelf-stacker Koyair could have had such a vast sum in their house.* (Sullivan 2006, emphasis in original)

Clearly, the story of the cash was intended to make the targeted family look suspect and justify the raid – to produce an anomalous association between the 'modest home', the 'shelf stacker' and 'the fortune'. The next day, however, it was revealed that the cash was the accumulated savings of the family, which they were 'reluctant to store in a bank because they felt that to do so would conflict with their religious beliefs'. It was also revealed that one family member had told police about the money only hours after the raid (Muir 2006).

This exemplifies the more prosaic prejudices concealed in the actions taken on the basis of the minutiae of daily life. The legal space of exception so notable in Guantanamo Bay and other contested spaces in the war on terror have their mundane counterparts in asset-freezing, preemptive arrest and no-fly lists. These mundane spaces of exception constitute not so much a reinsertion of surveillant state power into transnational business practice, but more a complex space of governing where commerce and security become mutually implicated in a myriad of ways. At the same time as constituting suspicious identities in relation to financial and travel transactions data, these security practices constitute new commercial opportunities and consuming identities. As Philippe Le Billon writes,

> The mobilization of consumption politics via 'the war on terror' is not only about redrawing 'homeland security' around the borders of the consuming self. It is also about inserting the narrative of terror within everyday practices, disciplining citizens, and constructing the terrorist 'other' through the consuming self. (2006, 781)

We are concerned here with the political implications of the ways in which transactions data

ISSN 0020-2754

are deployed for security decisions, in order to question these practices in a number of ways. If the sovereign decision is conceived as made up of a plurality of forces – instead of a 'lightning strike' – this has the advantage, according to Connolly, of rendering visible 'strategic issues and sites to address for those who seek to introduce a robust pluralism into the ethos of sovereignty' (2005, 145).

One of the remarkable elements in the story of the cash found in the wrongly raided London house is that here it was not so much a set of suspicious transactions but the *absence of transactions* that was thought cause for suspicion. The responsible citizen/consumer subject leaves open, visible and verifiable the map of their daily transactions. The absence of transactions, or the 'electronic footprint', then, is increasingly framed as suspicious in itself (Curry 2004), as it is thought to demonstrate transcience or a 'disembedding' from society. This is why, for example, informal money remitting services such as *hawala* are thought to be inherently suspect in the context of the war on terror: because they do *not* necessarily produce sets of transactions data preemptively accessible to security authorities (de Goede 2003; Atia 2007). This logic begins to demonstrate why *privacy* as a political concept is insufficient to politicise such new security practices. It is not just the case that most of us would not object to 'being seen' through the registration and analysis of our transactions. It is moreover the case, as Jordan Crandall (2005) points out, that modern life is impossible without it (cf. Stalder 2002, 122). If a record of one's financial transactions, travel data, insurance payments, etc. becomes like a credit-rating scorecard of one's embedding in society, not-being-seen is simply not an option. As Crandall puts it,

> Being-seen is an ontological necessity; we strive to be accounted for within the dominant representational matrices of our time. We are not only talking about a gaze that is intrusive and controlling. We are talking about a gaze that provides the condition for action – the gaze for which one acts. (2005, 20)

Thus, the call that rings out across the social sciences, for critical attention to the emergent 'global surveillant assemblage' that has intensified post 9/11 (cf. Lyon 2003; Haggerty and Ericson 2000), may be insufficient to politicise the geographies of transaction we discuss here. First, privacy itself restates the unity of the subject that is intrinsic to the preemptive strike we describe. Put simply, where the military preemptive strike assumes a nation-state, a citizenry, an identity that is securable, can be secured, the idea of privacy itself imagines an individual whose private data can be secured and made secret. Indeed, the original expert in transactions data mining, Rakesh Agrawal, demonstrates the ease with which privacy can be incorporated into the calculation. Now working for Microsoft, Agrawal has already moved to address the principal political objections to the use of algorithmic data mining in the war on terror: impacts on privacy and civil liberties. In his 'humane data mining' measures, Agrawal (2006) demonstrates how the identity of the individual connected to the data can be concealed to remain anonymous until a risk is flagged. The imagination of a world that can be secured through a particular calculative approach to data is scarcely interrupted by the appeal to make private the traces of our lives in our transactions.

Perhaps, bringing us to our second point, it is not so much a lack of privacy that is the political problematic, but rather a lack of social space in which we can see and be seen, engage with the differences and difficulties of our world. As the American novelist Jonathan Franzen writes: 'the networked world as a threat to privacy? It's the ugly spectacle of a privacy triumphant', 'we are flat out drowning in *privacy*' (2002, 50). What is absent, as Franzen sees it, is not strictly the possibility for privacy – this he sees as the guiding principle of a data-driven world where the encounters, differences and difficulties of public space are effaced by 'the right to be left alone' – but rather the ability *to be visible* in public space. To illustrate our point, at the same time as the minutiae of our daily transactions in the spaces of mall, subway or city plaza become ever more visible to security authorities of many kinds, our ability to simply walk around, to see and be seen in public space diminishes. The practice of *accounting* for us via our transactions paradoxically makes us *count* less in Crandall's and Franzen's terms of having a political engagement with the world around us. Our daily lives become a visible resource to geopolitics at the same time as we are rendered invisible in the geopolitical calculations made on their very basis.

Finally, we have argued that the actions taken on the back of screened transactions data do not constitute decisions, at least not responsible decisions that confront the contingency and uncertainty of how they may play out. This effacing of responsibility is

ISSN 0020-2754

partly due to technologies of consulting and calculation that render complex and indeterminate security decisions programmatic. They deny the difficulty, the very impossibility of some of the security ambitions. The effacing of responsibility is also underpinned by the vision of the worst-case scenario, 'too awful to contemplate'. As David Runciman asks

> Should worst-case scenarios, if they are sufficiently terrible, trump all other considerations when politicians have to decide what to do? . . . This stance . . . does not take seriously enough the downside of getting things wrong. (2006, 55, 57)

The downside of getting things wrong is visible across many domains of the war on terror, in the form of the wrongly shot, wrongly accused and wrongly targeted. The worst-case scenario makes it almost impossible to debate the role that preemptive action *itself* plays in shaping a contingent future, and has substantial power of justification of bad security decisions.

It is precisely this sense of responsibility in decision that we consider to be critical to future debates at the intersection of political and economic geography. If we are correct and the violent spaces of Abu Ghraib, Guantanamo, and extraordinary rendition have their more ordinary spatial counterparts in the prosaic places of the transaction, then we are all more directly implicated in authorising the preemptive strike. How is responsibility to be reintroduced to the decision, such that it confronts the political difficulties of indecision? A responsible decision would acknowledge the 'immersion of decision-making in the social and thus the impossibility of a sovereign state retaining a monopoly on decision' (Johns 2005, 632). It would take into account 'collateral damage', the 'mis-identified' and the 'false hit' as much more than accident or mistake, for it would be able to see how it risks bringing about the very futures it is supposed to predict. Rather as the military preemptive strike in Iraq has brought about links to al Qaeda that did not exist before the war (Richardson 2006, 166), so the targeting of transactions in the name of tracking terrorists brings about new forms of alienation and resentment. As Ericson writes,

> in its exceptional efforts to criminalize in response to uncertainty, the state helps manufacture malicious demons . . . [A]s selected populations are criminalized in ways that create terror, insecurity, injustice . . . [u]ncertainty ends up proving itself. (2007, 31, 35)

It is only by beginning a process of mapping and questioning the spatio-temporal and (geo)political logics of the banal face of preemption, we suggest, that the parameters and limits of the 'after 9/11' security decision can be more fully opened up.

Conclusion

We have argued that the deployment of everyday transactions, from the urban transit card swipe, to a credit card transaction, to a supermarket purchase, has taken on new meaning and significance in security practice after 9/11. The algorithmically projected transaction is thought to reveal a 'footprint' of the potential terrorist, which in turn is believed to enable preemptive security intervention. In fact, as we are working on this article, it is revealed that supermarket staff are being trained by British security services in how to detect potential terrorists. 'Extremist shoppers' are defined through their shopping transactions, and staff are taught to watch out for

> mass purchases of mobile phones, which can be used as bomb detonators [and] bulk sales of toiletries which could be used as the basic ingredient in explosives. (Goodchild and Lashmar 2007)

Again, transactions are imagined as a site where potential terrorists leave a footprint, while simultaneously the safeguarding of 'normal' shopping is positioned at the forefront of the way of life to be secured (Johnson 2002). In this logic, the mass purchase of mobile phones becomes a ground for preemptive security action, and possibly, a criminal offence in itself – as is the case with three Palestinian-Americans from Texas who were arrested in a Wal-Mart on the grounds of suspect shopping and are now awaiting trial (Goodchild and Lashmar 2007).

We have also argued that the mining of transactions data, and the preemptive security decision made on the back of that data, constitute a barely visible form of violence in the war on terror. While much critical literature is focused on the violence taking place in the war on terror's infamous spaces of exception, like Guantanamo and Abu Ghraib, a less visible violence, itself deeply implicated in rendition and detention, takes place through the articulation of new powerful definitions of normality and abnormality in transactions monitoring. Missing banking records, extremist purchases, suspicious travel paths all become grounds for abuse,

ISSN 0020-2754

questioning or detention. The violence of security action enabled by transactions monitoring pertains not just to the wrongly shot and wrongly arrested but resonates much more widely, as differential normalities become increasingly important for societal participation. As Samuel Weber puts it:

> Since the place targeted is always enmeshed in a net of relations that is intrinsically inexhaustible and unlimited ... the act of targeting is an act of violence even before any shot is fired. (2005, 105)

Finally, we have suggested political questions that need to be asked in relation to transactions monitoring and mining as a basis for security decisions. Data retention and mining are most often questioned and critiqued in terms of the politics of surveillance and individual privacy. Even if this is an understandable political move for those lawyers and activists who have to work within established juridical parameters, privacy as a critical concept is easily appropriated by data miners themselves, and, more importantly, reaffirms the logic of the isolated consuming individual to be secured. Instead, the idea of responsibility has to be reintroduced into the security decision itself. This means that preemption has to confront its own role in shaping the uncertain future. It means that preemption has to take into account the unpredictability of its *own* violence, and the exclusions and resentments that may produce the very thing it seeks to inhibit.

Acknowledgements

Many thanks to Adam Tickell and four anonymous referees for their very helpful comments on an earlier version of this article. We are grateful to the participants of the Geography seminar at the University of Durham in October 2006, where we presented some of this material, especially Ben Anderson, David Campbell, Rachel Colls and Stuart Elden. Special thanks to Paul Langley for his careful reading and his suggestion of our title.

Notes

1 On 26 September 2002, a Syrian-born Canadian citizen, Maher Arar, was detained by INS officers while in transit via New York's JFK airport. Separated from his family and denied legal representation, Arar was interrogated on his past travel and his associates. As 'evidence', the officers produced a rental lease he had signed in Ottawa in 1997. He was then chained and shackled and sent to Syria, where he was imprisoned and tortured for 12 months.

2 This example is drawn from the documented experiences of a participant in 'London in a Time of Terror', Birkbeck College, London, 8 December 2006.

3 The United States Visitor and Immigrant Status Identification Technology system of border controls screens data on individual transactions across multiple databases (Amoore 2006). See: http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (Accessed March 2007).

4 See Treasury's 'Counter Terrorist Financing Rewards Program' at: http://www.rewardsforjustice.net/english/index.cfm?page=Treasury (Accessed 19 September 2007).

5 Indeed, association with suspected terrorists or blacklisted persons becomes *itself* a crime through the criminalisation of terrorist financing and facilitation in the US and Europe. Under new anti-terrorist financing laws in the US, Laura Donohue (2006, 412) points out, 'mere associational links are sufficient to lose access to one's assets'. For an analysis of similar developments in Europe, see de Goede (2008).

6 In the UK context, for example, some premiership football clubs integrate the 'smart card' data swiped by season-ticket holders as they enter the stadium, with crime data held by police authorities. At one location, the swipe of an entry card will automatically flag child sex offenders to the CCTV security officers so that they may be identified by their seat number.

7 Ewald is talking about the precautionary principle here, and not premediation. There are many affinities between the logic of precaution, derived from imaginaries of environmental risk, and premediation, as they both emphasize the role of uncertain futures in imminent decisions. However, premediation draws attention to the representational practices – visual, textual, performative – that are always at the heart of 'imagining the worst'. For an examination of the logic of precaution in counterterror discourse, see Aradau and Van Munster (2007).

References

Agamben G 1995 *Homo sacer: sovereign power and bare life* Stanford University Press, Stanford CA

Agamben G 2002 Security and terror *Theory & Event* 5

Agamben G 2005 *State of exception* **Attell K** trans University of Chicago Press, Chicago IL

Agrawal R 2006 Humane data mining *Keynote speech at the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* Boston MA

Agrawal R, Imielinski T and Swami A 1993 Mining association rules between sets of items in large databases *SIGMOD Proceedings* 914–25

ISSN 0020-2754

Amoore L 2006 Biometric borders: governing mobilities in the war on terror *Political Geography* 25 336–51

Amoore L 2007 Vigilant visualities: the watchful politics of the war on terror *Security Dialogue* 38 139–56

Amoore L and de Goede M 2005 Governance, risk and dataveillance in the war on terror *Crime, Law and Social Change* 43 149–73

Amoore L and de Goede M 2008 Governing by risk in the war on terror in **Amoore L and de Goede M** eds *Risk and the war on terror* Routledge, London

Andreas P and Snyder T 2000 *The wall around the west: state borders and immigration controls in North America and Europe* Rowman and Littlefield, New York

Aradau C and van Munster R 2007 Governing terrorism through risk: taking precautions, (un)knowing the future *European Journal of International Relations* 13 89–115

Atia M 2007 In whose interest? Financial surveillance and the circuits of exception in the war on terror *Environment and Planning D: Society and Space* 25

Bennett J 2005 The agency of assemblages and the North American blackout *Public Culture* 17 445–65

Bigo D 2002 The Möbius ribbon of internal and external security(ies) in **Albert M, Jacobson D and Lapid Y** eds *Identities, borders, orders: rethinking international relations theory* University of Minnesota Press, Minneapolis MN 91–116

BMSA 2004 *The mathematical sciences' role in the war on terror* National Academies Press, Washington DC

Business Week 2001 The price of protecting the airways (http://www.businessweek.com/print/technology/content/dec2001/tc2001124_0865.htm) Accessed March 2007

Butler J 2004 *Precarious life: the powers of mourning and violence* Verso, London

Chertoff M 2006 A tool we need to stop the next airliner plot *Washington Post* 29 August A15

Connolly W E 2004 The complexity of sovereignty in **Edkins J, Pin-Fat V and Shapiro M J** eds *Sovereign lives: power in global politics* Routledge, London

Connolly W E 2005 *Pluralism* Duke University Press, Durham NC

Council on Foreign Relations 2007 The war on terrorism: the financial front Transcript 10 January (http://www.cfr.org/publication/12432/) Accessed 17 September 2007

Crandall J 2005 Envisioning the homefront: militarization, tracking and security culture *Journal of Visual Culture* 4 17–38

Crandall J 2007 'Readiness' and its formulas *Proceedings of the 'Architectures of Fear' Conference* Centre for Contemporary Culture Barcelona CCCB, Barcelona

Curry M R 2004 The profiler's question and the treacherous traveler *Surveillance & Society* 1 475–99

De Goede M 2003 Hawala discourses and the war on terrorist finance *Environment and Planning D: Society and Space* 21 513–32

De Goede M 2008 The politics of preemption and the war on terror in Europe *European Journal of International Relations* 14

Dean M 1999 *Governmentality: power and rule in modern society* Sage, London

Derrida J 1994 (in conversation with Richard Beardsworth) Nietzsche and the machine *Journal of Nietzsche Studies* 7 7–65

Derrida J 1999 *The gift of death* University of Chicago Press, Chicago IL

DHS 2006 *Survey of DHS data mining activities* Office of the Inspector General, Washington DC

Dodge M and Kitchin R 2005a Code and the transduction of space *Annals of the Association of American Geographers* 95 162–80

Dodge M and Kitchin R 2005b Codes of life: identification codes and the machine-readable world *Environment and Planning D: Society and Space* 23 851–81

Dodge M and Kitchin R 2006 Software and the mundane management of air travel *First Monday* 7

Donohue L K 2006 Anti-terrorist finance in the United Kingdom and United States *Michigan Journal of International Law* 27 303–435

Edkins J, Pin-Fat V and Shapiro M J eds 2004 *Sovereign lives: power in global politics* Routledge, London

Elden S 2007 Rethinking governmentality *Political Geography* 26 29–33

Elmer G and Opel A 2006 Surviving the inevitable future *Cultural Studies* 20 477–92

Ericson R V 2007 *Crime in an insecure world* Polity, Cambridge

Ewald F 1994 Two infinities of risk in **Massumi B** ed *The politics of everyday fear* University of Minnesota Press, Minneapolis MN 221–8

Ewald F 2002 The return of Descartes' malicious demon: an outline of a philosophy of precaution in **Baker T and Simon J** eds *Embracing risk: the changing culture of insurance and responsibility* University of Chicago Press, Chicago IL 273–302

Foucault M 2007 *Security, territory, population: lectures at the Collège de France 1977–1978* **Burchell G** trans Macmillan, Basingstoke

Franzen J 2002 *How to be alone* Fourth Estate, London

Goodchild S and Lashmar P 2007 MI5 trains supermarket checkout staff *The Independent* 30 March online edition

Graham S 2005 Software-sorted geographies *Progress in Human Geography* 29 562–80

Gregory D and Pred A eds 2007 *Violent geographies: fear, terror, and political violence* Routledge, New York

Grusin R 2004 Premediation *Criticism* 46 17–39

Guild E and Brouwer E 2006 The political life of data: the ECJ decision on the PNR agreement between the EU and the US *CEPS Policy Brief* 109 (http://www.libertysecurity.org/IMG/pdf/1363.pdf) Accessed 10 December 2007

Haggerty K and Ericson R V 2000 The surveillant assemblage *British Journal of Sociology* 51 605–22

Johns F 2005 Guantánamo Bay and the annihilation of exception *The European Journal of International Law* 16 613–35

Johnson R 2002 Defending ways of life: the (anti) terrorist rhetorics of Bush and Blair *Theory, Culture & Society* 19 211–31

ISSN 0020-2754

Kang J 1998 Information privacy in cyberspace transactions *Stanford Law Review* 1193 1198–99

Katz C 2007 Banal terrorism in **Gregory D and Pred A** eds *Violent geographies: fear, terror, and political violence* Routledge, New York 349–61

Le Billon P 2006 Fatal transactions: conflict diamonds and the (anti)terrorist consumer *Antipode* 38 778–801

Levitt M 2004 Untangling the terror web *SAIS Review* xxiv 33–48

Lyon D 2003 *Surveillance after September 11* Polity Press, Cambridge

Lyon D and Bennett C 2008 Card cartels in **Lyon D and Bennett C** eds *Playing the identity card* Routledge, New York

Martin R 2004 America as risk/securitizing the other *Interventions* 6 351–61

Massumi B 2005 *Parables for the virtual* Duke University Press, Durham NC

Massumi B 2007 Potential politics and the primacy of preemption *Theory & Event* 10

Muir H 2006 Terror raid family accuse police of slur over cash discovery *The Guardian* online edition 16 June

Prozorov S 2005 X/Xs: toward a general theory of the exception *Alternatives* 30 81–112

Richardson L 2006 *What terrorists want* Random House, New York

Runciman D 2006 *The politics of good intentions* Princeton University Press, Princeton NJ

Salter M 2008 Risk and imagination in the war on terror in **Amoore L and de Goede M** eds *Risk and the war on terror* Routledge, London

Shapiro M J 2007 The new violent cartography *Security Dialogue* 38 291–313

Snow J 2006 Financial intelligence *Washington Post* online edition 14 April

Sparke M B 2006 A neoliberal nexus: economy, security and the biopolitics of citizenship on the border *Political Geography* 25 151–80

Stalder F 2002 Opinion: why privacy is not the antidote to surveillance *Surveillance & Society* 1 120–4

Stanley J 2004 *The surveillance-industrial complex* American Civil Liberties Union, New York August

Sullivan M 2006 Raid brothers' £38K stash *The Sun* online edition 15 June

Suskind R 2004 *The price of loyalty* Simon & Schuster, New York

Taylor J B 2007 *Global financial warriors: the untold story of international finance in the post-9/11 world* WW Norton, New York

Thrift N and French S 2002 The automatic production of space *Transactions of the Institute of British Geographers* 27 309–35

Transport for London 2006 New deal brings Oyster and Barclaycard onto one card (http://www.tfl.gov.uk/corporate/media/newscentre/3746.aspx) Accessed March 2007

US Department of Justice 2002 *Hearing on the financial war on terrorism and the administration's implementation of the anti-money-laundering provisions of the USA PATRIOT Act* US Senate Committee on Banking, Housing and Urban Affairs, Washington DC

US Joint Inquiry 2003 *Report of the Joint Inquiry into the terrorist attacks of September 11, 2001* House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI), Washington DC

Walters W 2002 Mapping Schengenland, denaturalizing the border *Environment and Planning D: Society and Space* 20 561–80

Weber S 2005 *Targets of opportunity: on the militarization of thinking* Fordham University Press, New York

Zarate J C 2004 Bankrupting terrorists *E-Journal USA The Global War on Terrorist Finance* September

ISSN 0020-2754