Data wars beyond surveillance: opening the black box of SWIFT

Wesseling, M.; de Goede, M.; Amoore, L.

DOI
10.1080/17530350.2012.640554
Publication date
2012
Document Version
Final published version
Published in
Journal of Cultural Economy

DATA WARS BEYOND SURVEILLANCE
Opening the black box of Swift

Mara Wesseling, Marieke de Goede and **Louise Amoore**

This article examines the Terrorism Financing Tracking Programme (TFTP), or 'Swift affair,' as exemplary of what have been called 'Data Wars' in this special issue. In the TFTP, access to data about global financial circulations was offered as a means to govern uncertain security futures. The article endeavours to open the 'black box' of the Swift programme, by showing how *the Swift data were handled, accessed and analysed. We use the social science analogy of the black box as developed by Donald MacKenzie, but also because the datasets transferred from Swift to the US Treasury were in encrypted form, which literally came to be called a* black box*. In this paper, opening the black box has a dual meaning: both to reveal and reassemble the processes, procedures and analytical software tools of the TFTP, and to explicate a number of ethical, political and societal questions brought about by the programme. To open up the black box of this data war, then, is to push critique beyond the 'righting of the wrongs' (for example, to better protect data or to strengthen privacy), and to ask instead what such practices make of us and our world.*

KEYWORDS: SWIFT; financial intelligence; terrorism financing; black box; datamining

Financial information is 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. (David Aufhauser, in Council on Foreign Relations 2007)

It's like a TV, you don't need to know how it is built; you just want to watch your favourite shows. (EU Commission official, CEPS 2008)

Introduction: Swift and the Data War

On June 23, 2006, the *New York Times* disclosed the existence of the Terrorist Financing Tracking Program (TFTP) that had been initiated by the US Treasury and the CIA in the aftermath of 9/11. In the context of this programme, the Treasury requested and analysed financial records held by the Belgian-based Society for Worldwide Interbank Financial Telecommunication (SWIFT), that executes wire transfers on behalf of the global banking industry. The *New York Times* noted how the programme 'grew out of the Bush administration's desire to exploit technological tools to prevent another terrorist strike' (Lichtblau and Risen 2006). According to the *Los Angeles Times*, which publicized the existence of the TFTP later on the same day, this programme went far beyond earlier initiatives to access financial data for security purposes, in that it enabled security officials to 'follow suspicious financial trails around the globe . . . without having to seek assistance from foreign banks' (Meyer and Miller 2006). In the TFTP, access to data about global

Journal of Cultural Economy, Vol. 5, No. 1, February 2012
ISSN 1753-0350 print/1753-0369 online/12/010049-18
 http://dx.doi.org/10.1080/17530350.2012.640554
Routledge
Taylor & Francis Group

financial circulations was offered as a means to govern uncertain security futures. As one US official associated with the programme put it, financial data are 'extremely useful' because 'the evidence that the financial system coughs up is actually true and correct; it doesn't lie' (Aufhauser, in Council on Foreign Relations 2007).

The TFTP, or 'Swift affair', is exemplary of what have been called 'data wars' in the introduction to this special issue, as it involves a turn to existing commercial data and databases which are inscribed with the ability to map diffuse terrorist networks and reveal plots in preparation. Here, the languages and techniques of data analysis mirror the architecture of contemporary warfare in the ambition to identify, destabilise and incapacitate the nodes of fluid enemy networks in ways that simultaneously ensure the continuation of the daily lives of global finance (DerDerian 2001; Graham 2008). As we have argued elsewhere, such financial analyses promise a 'smart' form of targeting that mirrors and complements the logic of targeted killing and drone attacks (Amoore and de Goede 2011; Kessler and Werner 2008). In this context, a large number of international initiatives has been taken to enable the deployment of financial data and financial measures for security purposes, including the increased use of blacklisting and smart sanctions, the intensification of suspicious transactions reporting, and the targeting of informal transnational money flows (see for example Amicelle and Faravel-Garrigues this volume; Godhino 2010; Sullivan & Hayes 2010; Warde 2007; Vlcek 2008; Levi and Gilmore 2002). The Swift affair has to be understood in the context of this larger finance-security assemblage (de Goede 2012a).

This article examines in detail the Swift case as an empirical example of the contemporary data war. We endeavour to open the 'black box' of the Swift programme, by showing, as far as is possible within the constraints of significant public secrecy, *how* the Swift data were handled, accessed and analysed. We use the social science analogy of the black box as developed by Donald MacKenzie, for whom 'black boxes are devices, practices, or organizations that are opaque to outsiders because their contents are regarded as ''technical''' (2005, p. 555). MacKenzie has argued that it is important for social science to open the black boxes of finance, because it is precisely the representation of an arcane world of scientific devices that render it impossible to talk about or discuss. In the TFTP case, the datasets transferred from Swift to the US Treasury were done so wrapped in the technical sheen of protected and encrypted forms, which literally came to be called a *black box*. The data requested by the US Treasury – for example, all wire transactions from country X to country Y during a specific period of time – were provided by Swift in a so-called black box. Subsequently, the US Treasury mined and analysed the black-boxed data on the basis of specific search queries (Belgian Privacy Commission 2006a, p. 5). In our paper, opening the black box has a dual meaning: both to reveal and reassemble the processes, procedures and analytical software tools of the TFTP, and to explicate a number of ethical, political and societal questions brought about by the programme. As MacKenzie puts it, 'to sit on top of black boxes' is a very powerful position in modern societies (see Callon and Latour 1981). To open the black box of Swift, then, intends both to render (more) visible the technical processes of data and decision of this security programme, and to contribute to questioning its power. The Swift case embodies the data war's distinctive capacity to make actionable security decisions whilst simultaneously concealing these within a techno-scientific frame. To open up the black box of this data war, then, is to push critique beyond the 'righting of the wrongs' (for example, to better protect data or to strengthen privacy), and to ask instead what such practices make of us and our world.

Anchoring the Dispersed Enemy

The TFTP has to be understood in the context of a wider post-9/11 turn to commercial and financial data, which became inscribed with the capability of visualising terrorist networks and revealing 'blueprints of terrorist organisations' (Zarate 2004). Derek Gregory (2004) discusses the 'imaginative geographies' that visualise the new terrorist enemy. Two specific 'cartographic performances' were particularly important for Gregory in the run-up to the Afghanistan invasion: first, the imagination of Afghanistan as a coherent, sovereign state, and secondly, the 'performance of a territory through which the fluid networks of al-Qaeda could be fixed in a bounded space' (Gregory 2004, p. 50; compare Shapiro 2009). Here, the 'homeland' under attack was explicitly contrasted to the bounded, sovereign space of Afghanistan, that could be subject to a military campaign. As Gregory (2004, p. 50) concludes, 'it was an extraordinary accomplishment to convince a sufficient public constituency that these transnational terrorist networks could be rolled into the carpet-bombing of Afghanistan' (see also Elden 2007, Campbell 2002).

However, it can be argued that emphasising the deterritorialised, dispersed and global nature of contemporary terrorist networks entails its own spatial imaginations, that are not reducible to a specific geographical territory, but that foster important visualisations of the enemy and enable localised security actions nonetheless. Understanding al Qaeda as a 'network of networks, with neither capital nor center' (Gregory 2004, p. 50) is itself an important spatial imagination, closely related to a particular understanding of contemporary warfare and the dispersed nature of the post-9/11 enemy. A number of authors have drawn attention to the ways in which security establishments conceive of the contemporary threat as globally dispersed, urbanised, mobile and a-symmetrical (see DerDerian 2001; Graham 2008; Coward 2009; Anderson 2011). In the face of this new type of networked and sub-state threat, governments have to 'adopt organizational designs and strategies like those of their adversaries,' because, as Arquilla and Ronfeldt (2001, p. 15) put it in their popular soundbite, 'it takes networks to fight networks.' Consequently, as Graham (2008, p. 37) shows, network-centric warfare offers a vision of 'a new, relatively reduced-risk, ''clean'' and painless' strategy of military dominance that partly operates on the back of a reconceptualisation of the urban terrain as a site of combat.

Post-9/11 terrorism is conceptualised as the epitome of this new networked threat, especially through influential diagnoses of the so-called 'new terrorism' marked by the triple features of a 'universalistic ideology,' a 'world wide network of operational and preparative cells,' and the 'nature and scale of the violence [it] employs' (Wilkinson 2003, p. 3–4; also Ranstorp 2007). Discourses of the new terrorism in academic circles are closely interwoven with increasingly important notions of sleeper cells, homegrown terrorists and jihadist 'self-burners,' that form an important element in post-9/11 policy reports (for example, Chesney 2005). Marc Sageman (2008, p. 37), for instance, sums up his understanding of the contemporary threat of terrorism as follows: 'the new generation of terrorists consists of homegrown wannabes – self-recruited, without leadership, and globally connected through the internet.' Such formulations have made their way into key policy documents, including the 2010 Trends and Terrorism report of Europol, according to which the current threat to the EU 'is increasingly likely to originate from self-radicalised individuals and a diversity of militant extremist groups, including those who are, or claim to be, affiliated with al-Qaeda as a movement, rather than linked to AQSL (*al-Qaeda's senior leadership*) on a personal level' (Europol 2010, p. 20).

Yet, it is not merely the representation of a network of dispersed and loosely affiliated terrorist groups that makes possible the financial data war. Rather, it is the perhaps more mundane imaginary of a global financial network of transactions, centres, nodes and circulations that appears to offer up a distinctive potential for security intervention. In the networked imaginary of global financial transactions, one might say, are the material instantiations of a much more nebulous and ideas-based terrorism network. As one journalist observer put it, 'maybe we can't cut off terror's head, but we can take out its nodes' (Garreau 2001). Following-the-money and examining transaction trails have become one method in the drive to identify the nodes of complex, moving and diffuse terrorist networks. This is expressed in the idea of the 'financial footprint' that is supposedly left behind through the mundane transactions that precede violent acts. As one US Treasury official has put it: 'Terrorists and their supporters leave identifiable and traceable footprints in the global financial systems, and these footprints must be pursued forward to identify *future perpetrators and facilitators*' (Zarate 2004; see also Hall and Mendel, this volume). In summary then, images of the networked enemy and asymmetric warfare work to securitise not just urban territories, but also the less visible architectures of daily life in general and the everyday life of global finance in particular (Langley 2008).

Opening the Black Box of Swift

The TFTP, or Swift affair, is one of the most important, visible and contested instances in which mundane financial data were deployed for security analysis (also Amicelle 2011; Amicelle and Faravel-Garrigues, this volume). However, to date there has been very little investigation of the operational and technical aspects of the TFTP, with scholarly and societal attention focused on the programme's implications for privacy and civil liberties (see, for example, de Hert and de Schutter 2008; Gonzalez Fuster, de Hert and Gutwirth 2008; Belgian Privacy Commission 2006b; 2008). This lack of analysis of the technologies and analytical practices in the Swift case can only be partly explained by a lack of publicly available knowledge of the content of the programme – which remains officially classified at the time of writing. Virtually all of the 7800 banks submitting their clients' data to the Swift system were unaware of the potential communication of this confidential information to the US Treasury until disclosure of the programme by the *New York Times* in 2006. Only a few selected members of the US Congressional and Senate committees on security and intelligence were informed about the TFTP in 2002 and some others in spring 2006 when the *New York Times* indicated that it would publish the story (Lichtblau 2009, p. 254). However, on the basis of official statements, debates and interviews, it is now possible to retrieve and reassemble knowledges concerning the analytic techniques deployed in the Swift case and their parallels to other cases of the contemporary data wars.

Two further factors can be said to be at work in our lack of public knowledge concerning the mode of operation of the TFTP more than five years after its disclosure. First, there was a substantial reluctance by a number of institutions that *did* know about the programme, for example the European Central Bank, to claim competence over the issue and initiate its own investigations. National data protection agencies, as well as the European Data Protection Supervisor, do not have the power to investigate a case and hear people beyond the territory for which they are competent. For this reason, even the Belgian Privacy Commission, which had taken the lead in investigating the transfer of Swift

data, was not able to monitor the data transfers and analysis in the US (interview with the Belgian Privacy Commission). In brief, it is more than official secrecy that is at work in the lack of public knowledge of the technical details of our contemporary data wars: it is also the result of a minimization of competence over what is potentially an explosive political issue.

Secondly, the TFTP, like other aspects of contemporary data wars, entails a promise of a technological 'fix' to complex security challenges. It is seductive for policy-makers and security officials to believe that inquiring into the practices of the TFTP in detail is irrelevant as long as it 'works' and generates leads and security action. As an official from the European Commission put it with respect to the reliability of DNA profiles: 'it's like a TV, you don't need to know how it is built; you just want to watch your favourite shows' (CEPS 2008). The specific techniques deployed to gather, integrate, mine and analyse the data are thus afforded less political significance than the effects – the watching of the 'show'. However, the new methods for investigation and intelligence gathering at work within the TFTP and through the new availability of financial datasets have the potential to resonate beyond the Swift case and are exemplary of larger shifts in contemporary surveillance and data wars. This point is confirmed by a former senior counter terrorism official who stated: 'the capability here [of the TFTP] is awesome or, depending where you're sitting, troubling' (quoted in Lichtblau and Risen 2006). The introduction of the TFTP silently allows radical changes regarding a number of democratic principles and judicial safeguards. On both sides of the Atlantic, the TFTP has been transformed from an illegal or at least a questionable surveillance programme, in which judicial and congressional overview were absent, into a legitimate and legal programme without any (legal) consequences for the parties involved (de Goede 2012b).

As a consequence, it is important to enquire into the technological processes underpinning contemporary data wars and to open the black box of security programmes like the TFTP. When it comes to the techniques of surveillance and security, authors including Elia Zureik and Mark Salter (2005, p. 5) have argued that examination of 'paths, processes and institutions of the movement of data and information' are equally important to studying the movement of people and of money flows. In other words, we need to understand more precisely the trajectories of commercial data, collected for the purpose of facilitating business transactions, as they become reassembled and inscribed with new meanings in the context of security practice. How and where did these data become unmoored from their commercial purpose and inscribed with new meanings? How were datasets assembled in the face of the Treasury subpoenas? How were these (black-boxed) datasets moved and objectified? How were they examined, mined and visualised? And how did this lead to new modes of actionability? Bruno Latour (1999) has offered the concept of 'circulating reference' to analyse the social practices whereby information is produced and science is made (see also Latour 2005). Such circulating reference, for Latour (1999, p. 26), involves a highly social and partly contingent process whereby 'a small part of the forest of Boa Vista' is selected, collected, transported, translated, inscribed – but also left, forgotten and lost – in order to produce scientific meaning concerning global climate change. The relationship between object and words, or more generally, material stuff and scientific conclusion, in this analysis, follows a 'risky intermediary pathway' (p. 40). Without claiming that we are able to do for TFTP what Latour does for the research on Amazonian soil which he studies, we will take his cues and attempt to retrace in some detail the processes of inscription, selection, transportation,

translation and signification of data at work in the TFTP. The intermediary pathway between the 'stuff' of data and the actionable conclusions from the TFTP analytic, we suggest, is even more risky than that of Latour's soil scientists. This is not so much because the stuff of data is less material, but more because the interpretative steps and technical reassemblages at work within the TFTP are more self-consciously speculative. Our approach, then, intends to render visible both how financial data are redeployed and re-inscribed with new meanings and the riskiness of such interpretative force, that is wholly masked by the injunction that 'money trails don't lie.'

The particular interest of intelligence and law enforcement agencies for the data held by Swift did not arise after the 9/11 attacks. Already at the beginning of the 1990s, under the administration of George Bush senior, the US government tried to obtain information from Swift via traditional subpoenas issued by the US Treasury Office of Foreign Assets Control (OFAC). For authorities, the attraction of the Swift database was perceived to lie in the fact that it constitutes an information hub of a very large part of the financial sector (the company handles about 80% of the financial transfers worldwide). Law enforcement officials were interested to search through the Swift database because it unites transactions of thousands of banks in one system instead of issuing separate requests to individual banks. In the 1990s, requests by US authorities for access to its database were not granted by Swift, which argued that the data could more easily be obtained through the sending or receiving bank, or because the demand implied a name search which is impossible in the Swift system (Belgian Privacy Commission 2006a, p. 5).

Throughout the 1990s, pressure was put on the company by the US Justice Department to include more elements of financial data in their messaging system and to make deciphering the Swift's encrypted data easier. The Justice Department also asked for access to broader sets of financial information from Swift's database to support criminal investigations. In those years, but also just after 9/11, the CIA had even considered secretly entering the SWIFTFin NET service (Lichtblau 2009, p. 243). Swift's resistance to cooperating with law enforcement changed after the 9/11 attacks. Reminded of Swift's database being 'the mother lode', 'the Rosetta stone for financial data' by a Wall Street executive (quote in Lichtblau and Risen 2006), the Bush administration decided to approach Swift again. This time, Swift's American CEO Leonard Schrank, who felt very much affected by the 9/11 attacks, was keen to cooperate (Lichtblau 2009, pp. 234, 243).

The way in which the TFTP operated was through the issuance of subpoenas by the US Treasury to Swift's US-based processing centre (which retained copies of all data for 124 days), requesting access to specific categories of data. Since the Swift messenger service doesn't have a research tool in its operating centre for queries concerning names or other personal data, Swift could not directly deliver the data elements requested by the CIA (Belgian Privacy Commission 2006a, pp. 5, 10). To make matching between the CIA lists of suspected terrorist financiers and operatives and the Swift data possible, datasets were made available from Swift's mirror database to the US Treasury. These datasets were literally called the 'black box.' They contain all the messages responding to criteria requested in the subpoena; for example, all transactions within and outside the US to particular countries and jurisdictions, on a specific date or in a specific period of time, ranging from one day to several weeks. The CIA analysts requested data concerning more than thirty countries involved in terrorism financing including Saudi Arabia, Pakistan and the United Arab Emirates (Lichtblau 2009, p. 244). To consult the data the US Treasury designed search software to decrypt and consult the messages in the black box on the

basis of specific searches by name. The Belgian Privacy Commission concludes from its investigations that the 'number of subpoenaed messages must be enormously high,' given the daily message traffic via SWIFTNet FIN of approximately 11 million messages in 2006 and over 2.5 billion messages on a yearly basis in 2005 (Belgian Privacy Commission 2006a, pp. 5–6).

The transfer of data from Swift's database to the US Treasury started within two weeks of the terrorist attacks of September 11 2001. Initially, the US authorities were given unlimited access to the Swift database, although according to statements by Swift, the US Treasury and the CIA were never given a full copy of the SWIFTNet FIN database. Later, monthly administrative subpoenas were issued by the US Treasury to Swift's American operation centre in order to obtain the black box and give SWIFT an element of proof that it had no choice but to cooperate with US authorities.[1] It would have been possible to challenge the subpoenas in court, like Swift had done before 9/11, but the company chose not to. Nevertheless, the nature of these subpoenas was problematic in that they were qualified by the Belgian Privacy Commission (2006a, p. 5) as extremely broad 'non individualised mass requests' permitting the indefinite monitoring of certain financial transaction flows.

Once extracted from the Swift system, blackboxed and transported to the US Treasury, the data became inscribed with new meanings and visualised in particular ways. According to Stuart Levey, former Treasury Undersecretary of Terrorism Financing and one of the initiators of the TFTP: 'The way Swift data works, you would have all kinds of concrete information – addresses, phone numbers, real names, account numbers, a lot of stuff we can really work with, the kind of actionable information that government officials can really follow up on' (quoted in *Washington Post* 2006a). Various sources confirm that the data were deployed for what is called 'link analysis' or 'social network analysis,' whereby the relationships and connections of suspect individuals or entities are traced and mapped. The *LA Times* quotes unidentified Swift officials who say that the data were used for link analysis:

> That technique allows analysts to identify any person with whom a suspected terrorist had financial dealings – even those with no connection to terrorism. That information is then mapped and analyzed to detect patterns, shifts in strategy, specific 'hotspot' accounts, and locations that have become new havens for terrorist activity. (quoted in Miller and Meyer 2006)

The Belgian Privacy Commission (2006a, p. 5) notes that automated *searches of names* were conducted within the black-boxed data. Presumably, these were the names of the 9/11 hijackers, and others on terrorism blacklists including the official UN and US terrorist lists imposed by UNSC resolutions 1267 and 1773. On these lists, al Qaeda-related individuals and entities are included but also other suspected terrorists and terrorist organisations. However, at least in theory, there should be no or very few hits with these names in the Swift database since it is legally forbidden to make a bank transfer or provide any other financial service to listed individuals and entities, and their assets should be frozen. Therefore, it is very probable that broader watch lists have been 'flushed through the system' (see also Amicelle 2011). Like other intelligence services, the CIA has access to the Terrorist Identities Datamart Environment (TIDE) containing data on known or suspected international terrorists. According to the American Civil Liberties Union (ACLU), this watch list of terrorism suspects has over a million records corresponding to

approximately 400,000 people in 2008 (Reuters UK 2008) and it is continually expanding (see for example Sullivan 2010). This watch list information also includes separate entries with aliases, (fake) passport numbers and (fake) birth dates. The vast majority of the listed persons (95%) are not U.S. citizens or residents (Young 2007).[2] In the first five years of the programme tens of thousands, maybe hundreds of thousands, of financial transactions have been examined (*Washington Post* 2006b).

When a positive match occurs between the names held on the watch lists or in intelligence documents and the Swift data, for instance through a real name, an alias, or a bank account number, analysts seek to map all those with whom the person conducts financial transactions. Although the details on the methods used to produce intelligence from Swift data remain secret, it is known that the FBI conducts link analysis up to three or four links removed from the initial suspect, and the CIA even goes up to five or six links (interview by the authors 2010). Link analysis has become a key security technique in the context of so-called 'netwar'. It is thought to be possible to 'connect the dots' between individual terrorists, and so to anchor and visualise a dispersed, global, mobile and networked enemy. One of the first to produce visualisations of the 9/11 hijackers' social network was consultant and software developer Valdis Krebs, who published elaborate network images with more than one hundred 'associates' of the hijackers, as well as correlated events such as the bombing of the USS Cole (see Krebs 2002; Krebs n.d.).

We have to understand, however, that link analysis can be understood as a purposefully speculative technology with the objective of broadening the universe of suspects and the scope of law enforcement investigations. Deploying link analysis means that, from the basis of particular suspects, a financial data 'string' may be 'pulled', in order to associate names, phone numbers, social security numbers, credit card numbers and addresses from different databases. We know that the names of perpetrators and suspects of all major post-9/11 terrorist events were flushed through the Swift database, including for example those of the 2002 Bali bombings, the 2004 murder of Dutch filmmaker Theo van Gogh, the 2004 Madrid Train bombings and the Mumbai attacks of 2008. In all of these cases, the objectives were to widen investigations, draw in new suspects and identify associates and potential future terrorists. Recently, it has been revealed that US authorities shared over 1,550 potential investigative leads with their European colleagues (Cohen 2010). Such investigative leads might simply imply passing on a name or other data elements without further information except the advice to look into this case. The reality of the searches into the black box thus might have been messier than appears in the description above. According to an official 'this was creative stuff, nothing was clear cut, because we had never gone after information this way before' (quoted in Lichtblau and Risen 2006). In the creativity of the network produced through link analysis, then, is the capacity to infer possible connections and to speculate about their future intent. Analytical techniques such as social network analysis and link analysis do more than mine existing data in new ways: they actively reassemble the data, inscribe them with new meanings and project potentialities for intervention.

In the next section, we conceptualise in more detail the techniques of visualisation and projection at work in the TFTP and related programmes. Here, it is intriguing to note that there has been little publicity about the 'success stories' of a programme that ran 24/7 and is continuously described as a vital tool with 'tremendous' possibilities (e.g. *Los Angeles Times* 2006). The press articles revealing the Swift affair in June 2006 mention only one high profile case, that of Riduan Isamuddin, alias Hambali, the leader of Jemaah

Islamiyah (JI), a terrorist organisation linked to al Qaeda and allegedly the mastermind behind the 2002 bombing of a Bali nightclub and the 2003 attacks on the Jakarta Marriott hotel. According to the *New York Times* 'the SWIFT data identified a previously unknown figure in Southeast Asia who had financial dealings with a person suspected of being a member of al Qaeda, that link helped locate Hambali in Thailand in 2003' (Lichtblau and Risen 2006). Hambali was arrested in a joint operation of the Thai authorities and the CIA and subsequently brought to a secret prison (Human Rights Watch 2004). Later that year he was transferred to Guantanamo Bay. The second 'success' case on the basis of Swift data that has been publicly revealed is that of Uzair Paracha, who has been convicted for laundering $200,000 through a bank in Karachi to help an al Qaeda operative in Pakistan. Paracha was eventually sentenced to a 30-year prison sentence, and his July 2006 sentencing holds up the case as exemplary of the Department of Justice's commitment to 'proactive investigation' and 'aggressive prosecution.'[3] A third case in which Swift data is said to have played a role is a disrupted terrorist plot in the UK of the so-called 'liquid bombers'.

It remains to be seen whether these cases and recent figures justify the often repeated claims, such as those made by the Swedish EU presidency or former US Treasury Secretary John Snow, (*Washington Post* 2006a) that because of Swift 'lives have been saved.' In the words of one member of the European Parliament: 'It is a fairly bold claim and if it is true then it is an important fact but we would like to see it black on white. 'I want proof you know, we are decision makers, when we will be asked to take a decision on this I want all the facts and figures'. '[Evidence has not been forthcoming] because in some cases it is simply not there' (interview with a Member of the European Parliament). The examples that we do have, however, demonstrate clearly that the transportation, translation and inscription of the Swift data in the context of security practice has the ability to lead to real interventions including imprisonment in Guantanamo. The next section looks at the avenues of conceptualisation and politicisation of the risky intermediary pathway between data and intervention that we have attempted to unravel here.

Surveillance versus Projection

Enhanced datamining in the context of the war on terror, including the TFTP, suspicious transactions reporting, analysis of passenger name records and immigration databases, is often understood and critiqued in terms of 'surveillance' (e.g. Lyon 2003; Zureik and Salter 2005). Such readings emphasise the extent of (government) access to personal financial data authorities, and concomitant declines in data security and financial privacy. Post-9/11 financial datamining and the risk-based regime to suspicious transactions monitoring have fostered an unprecedented recoding, reviewing and analysing of ordinary, everyday financial transactions. In this respect, for example, William Vlcek (2008, p. 35) signals the emergence of a 'financial panopticon' and writes: 'the system of financial surveillance is increasingly global, sliding its tendrils into the financial and non-financial institutions of developed and developing states alike.' It is the *surveillance* of financial transactions that concerns Vlcek (2008, p. 29), which, in his reading, has 'metamorphosed' financial institutions into 'informants for the state.' Peter Shields (2004) similarly notes an increase in financial surveillance in which law enforcement extends its surveillance powers to new forms of financial transactions. Ibrahim Warde (2007), by comparison, speaks of a new system of 'gated finance' in which specific client

groups, firms and countries become excluded from the international financial system. Consequently, Warde suggest that this has effected a criminalisation of 'banking while Arab.'

However, our opening of the black box of the TFTP suggests that this programme does not necessarily operate as a practice of surveillance – if surveillance is understood as a more or less systematic capture and scrutiny of a wide range of financial transactions. Kevin Haggerty and Richard Ericson (2000) offer the term 'surveillant assemblages' to conceptualise the heterogeneous nature of contemporary surveillance and datamining. They resist the notion that surveillance originates from a single coherent point of observation, and document some of the points of cross-over by which commercial data become mined for policing purposes (also Ericson 2007; Levi and Wall 2004). The ways in which programmes like the TFTP depart from technologies of surveillance can be clarified by examining Foucault's distinction between *surveillance* as a paradigm of power that works through individual subjectification, and *security* as a paradigm of power that works on the population through the invention of statistical regularity (Foucault 2003, p. 2007). Surveillance presupposed 'putting someone in the centre – an eye, a gaze, a principle of surveillance – who will be able to make its sovereignty function over all the individuals,' wrote Foucault (2007, p. 66). Thus, for Foucault, 'the panopticon' can be said to be 'the oldest dream of the oldest sovereign.' Security, in contrast, is a 'completely different technique . . . that is not getting subjects to obey the sovereign's will, but having a hold on things that seem far removed from the population, but which, through calculation, analysis, and reflection, one knows can really have an effect on it' (p. 72). Security, in this sense, is a technique that works on the future through the compilation and classification of phenomena previously considered as 'accidents, chance, individual conduct, and conjectural causes' (p. 74).

Thus understood, the power at work in financial datamining operates through the paradigm of security – rather than that of surveillance – in which the objective is not to observe, prohibit and forbid, but to visualise, differentiate and allow (see also Amoore and de Goede 2008). More research needs to be done, but there is increasing evidence that other data-led security programmes including those based on passenger name records (PNR) depend on similar security techniques as the TFTP, in which particular visualisations and differentiations work to allow continued circulation (see also Sparke 2008). These programmes work through the redeployment of commercial data for link analysis, the mapping of association, and the generation of new leads for investigation and interception. Indeed, within the 'creativity' that is accorded to the use of Swift data, there are many data elements that become available for cross-matching or linking with data available from other sources. For example, the data fields proposed within the 2011 EU-US agreement on the transfer of PNR data include method of payment data and past travel data that, if it were to follow the techniques of programmes such as the USVISIT, would be available for integration with Swift data.[4]

While the data orientation of techniques of surveillance can be understood as one of *survey*, in which the subject is made governable through the collection of data on population, the security techniques of data wars are more akin to the *projection* of multiple data elements (Amoore 2011). Projections are produced from fragments of data, from isolated elements that are selected, differentiated and reintegrated to give the appearance of a visual whole. Thus, the purpose of financial link analysis as deployed in the Swift case is not to trace the steps and seize the assets of known criminals or

terrorists but to visualise networks of association and to identify the 'unknown terrorist.' According to the US Treasury's (2006) press release concerning the Swift affair, the data were deployed in order to 'map out terrorist networks' and for '*filling in missing links* in an investigative chain' (emphasis added). In a 2007 discussion, Aufhauser similarly reveals that the Swift program 'helped map out connections between people even through the most innocent of transactions, people that we might have had suspicions about and would therefore lead us into better definitions and understandings of cells and plots and conspiracies' (Council on Foreign Relations 2007; also Taylor 2007, pp. 19–20).

Unlike the survey in which decisions on sampling and accuracy are paramount, the decisions about what to select, how to isolate, what should be joined where and how, fall away in the appearance of a projected whole. In her discussion of filmic projection, Anne Friedberg suggests 'for motion to be reconstituted, its virtual reach relies on a missing element, a perceptual process that depends on the darkness between the frames' (2007, p. 92). Like filmic projection, the gaps between items of data are what makes an actionable security decision possible. For the suppliers of software and risk management solutions for terrorism financing tracking, border controls, immigration and customs, the focus is on what can be conducted 'across items of data' (software designer, interviewed 2009). What is not known thus becomes the basis for calculation. There can be no certainty about the association between a particular wire transfer, a method of payment, or a credit card number, for their relation is not causal. As the US Inspector General concluded in his review of the use of data analytics, 'association does not imply a direct causal connection ... but uncovers, interprets, displays, relationships between persons, places and events' (2006, p. 10). Because it is the very relation between associated data that becomes a flagged or suspicious element, it is of less importance whether a particular terrorist event is in preparation, what matters is the capacity to act on the future possibility. As Brian Massumi has put it, '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, pp. 7–8).

Indeed, precisely the fact that the Swift data were not used to survey vast tracts of the population was an important argument that was deployed by defenders of the programme. In the debates following the disclosure of the TFTP, government officials repeatedly insisted that the Swift information was never used for datamining: as one defender of the programme put it to the *New York Times*: 'we are not turning on a vacuum cleaner and sucking in all the information we can' (Lichtblau and Risen 2006). Stuart Levey has emphasised that the TFTP was 'not a fishing expedition but rather a sharp harpoon aimed at the heart of terrorist activity' (quoted in *Washington Post* 2006a). Here, (automated) link analysis is justified and deemed acceptable because it is believed to be finitely targeted on specific links – the CIA is not surveilling the whole database but undertakes specific searches on basis of a name from the watch list. However, it is important to stress that link analysis may involve enormous amounts of data too. First, the black box retrieved from the Swift database contains millions of data items: even if not all of these are extracted by authorities, they are nevertheless maintained for access for up to five years (under the new EU–US agreement). Second, the lists with terrorism suspects contain thousands of names. Third, the searches across relations between data items – up to six links separated from the initial suspect – are exponential in character leading to inferences that significantly exceed the initial name on a watchlist. If the FBI and the CIA start from just one person or entity and map all its financial connections, and

subsequently all the connections of the connections are also mapped, up to three or four steps of separation for the former and five to six for the latter, infinite numbers of data may still be involved.

More important than the precise amount of data accessed, moreover, are the larger political questions that arise in the context of the data war insofar it is not a practice of surveillance. These concern transformed modes of targeting and a novel logic of evidence and responsibility. Thus, the practices of the data war as it is fought through programmes such as the TFTP raise questions about targeting and the limits of the network. Departing from data from one individual, others that are part of his/her 'network' of financial transactions become part of the investigation. While this may include links to suspicious accomplices, it almost certainly also includes what some call 'pizza courier hits'; drawing very innocent daily transactions such as payments for rent, groceries or a pizza delivery into intelligence investigations. Furthermore, there is now public evidence of cases where charitable monies have been frozen mid-transit to disaster areas, although, of course, it is difficult to prove that these cases were directly linked to the TFTP (interview with Islamic Relief; see also Amoore and de Goede 2011; ACLU 2009). This is not only questionable from the perspective of privacy rights and efficiency, it also prompts us to consider the meaning of a network. This question has been discussed by legal experts[5] but it has so far received little attention with respect to the analytical tools of the data war. If perhaps the TFTP is not a matter of switching on the vacuum cleaner, sucking in and analysing all the information of the Swift database, it is also unlike a sharp harpoon, targeting and eliminating one specific prey. Once an individual is targeted it rather works as a *cluster bomb*, designed for targets not precisely identified and indiscriminately hitting anyone surrounding the initial target up to four or six links removed. Hence, like cluster bombs, link analyses or social network analyses have a wide area of effect through which they may 'hit the target' and be able to reveal financial relations between terrorists, but they also produce a lot of 'collateral damage' in the form of false positives and useless links. Moreover, defining whether the connection between the dots is actionable, and constitutes a hit, depends on the ability of financial investigators to (re)construct or imagine a posteriori the context and relevancy of a financial transfer.

Consequently, critical questions can be raised about the transformed legal landscape of security evidence and intervention. The main purpose of the TFTP, as we have seen, is to generate new targets within investigations, generate connections between suspects and to broaden the possible field of security intervention. Here is one example mentioned by Assistant Treasury Secretary Cohen in support of the TFTP in an April 2010 speech:

> In October 2008, eight individuals were arrested in Spain for their suspected involvement with al Qaeda. European partners provided us information outlining these individuals' suspected connection to terrorism, and TFTP information clarified connections between the targets and other individuals in Spain, Morocco, and the Netherlands. (Cohen 2010)

However, this example, as well as social networking technologies more broadly, raises significant questions concerning the evidentiary basis of wrongdoing and the logic of intervention. When and how does a monetary connection become grounds for investigation or disruption? What are the evidentiary bases for pursuit and arrest when such actions are taken on the basis of monetary connections? How can such security actions be accorded a measure of transparency and accountability? The new EU–US

agreement on the transatlantic sharing of Swift data now includes articles on the maintenance of accuracy of information and possibilities for redress. These articles are included with the purpose of guaranteeing, to European citizens, via their national privacy officers, administrative and judicial redress in case their data have been processed in breach of the Agreement.[6] But this clause may be largely symbolic when the programme and the processing of the data remain secret and the origin of the source is hidden when data are shared among law enforcement agencies. In addition, the agreement stipulates that transactions can be accessed and examined when there is a 'nexus' between the transaction and terrorism.[7] But the nature, breath and definition of what is meant by such a nexus remains unclear. If understood through the lens of projection and visualisation, the security practices of the war on terror give rise to new critical questions concerning the visibility, accountability and responsibility of targetings.

Conclusion: Politicisations

This paper has attempted to shed light on the data techniques deployed in the TFTP and has made some first steps at opening up its assumptions and logics to critical questioning. We have argued that the Swift affair is exemplary of the contemporary data wars because it seeks to visualise and anchor a dispersed, mobile enemy through novel deployments of data analysis that exceed what is conventionally understood as surveillance. Thus, the purpose of the TFTP has not been so much to collect, access and surveil *all* financial data of citizens, but, instead, to target, select and identify specific leads. The key difference between surveillance and projection is that the latter has a specific relation to the deployment of past data in relation to uncertain futures. Because it 'takes apart' and then reassembles in order to project future movement (like film does), it gathers some fragments of past actions or events (for example, financial data from the Madrid or Bali bombings), and associates these creatively with other fragments, patterns or data items. In this manner, the future is made actionable in a distinctive way in the present.

The move from surveillance to projection, from datamining to social network analysis, necessitates a novel politics for those wishing to raise critical questions about the logic of evidence and modes of responsibility enacted through such moves. If our reading is correct and the TFTP is less about surveillance than it is about projection, it follows logically that existing concepts of political contestation, including privacy and data protection, have limited critical potential in the face of these developments. For example, one of the concerns of the European Parliament in the face of the disclosure of the existence of the TFTP, was that of US security authorities trawling through private data of European citizens by accessing and mining large datasets of sensitive financial information. However, in response to this objection, it was not difficult for US authorities to promise *not* to engage in datamining, and to stipulate, in the June 2010 Treaty between the US and the EU on this matter, that 'the TFTP does not and shall not involve data mining or any other type of algorithmic or automated profiling.'[8] In a sense, to 'mine' data is to engage quite traditional techniques of delving for past data against specific criteria, such that information can be extracted to say something about the future. Social network analysis and other forms of analytics have a different relation to past data and future projection precisely because they generate possible futures from the relations between data items. In addition, link analysis has a different logic from that of profiling: it is not about the discovery of the properties of a particular group of financial clients, but about

the visualisation of the network relations of particular named individuals, addresses or credit card numbers. Thus, to promise not to engage in datamining is possible for US security authorities because that is *not* the analytical technique deployed with regard to the Swift data – if we understand datamining to involve looking for pre-established markers of suspicion or suspicious transactions patterns. Furthermore, under programmes like the TFTP or risk-assessments through passenger name records, it is relatively straightforward to render personal data private by anonymizing records and substituting names with code (see van der Ploeg 2003; Amoore and Hall 2009). In short, the 'dots can be joined' in the absence of definitive named persons because link analysis and associated techniques focus on the linking and not the dots. What is needed instead in the face of the financial data war is juridical and critical scientific attention to the gaps between the frames that make the projection possible, and a better understanding of how mundane details and transactions become assembled into markers of suspicion and incrimination.

ACKNOWLEDGEMENTS

Many thanks to two anonymous reviewers for their very helpful comments on this piece. Funding for the research of risk-based approaches to targeting money and people is provided by ESRC (UK) and NWO (Netherlands), DataWars: New Spaces of Governing in the European War on Terror, award number RES 062230594.

NOTES

1. The total number of subpoenas from the US Treasury received by SWIFT in June 2006 was 64 (Belgian Privacy Commission 2006a).
2. The TIDE database is used to compile various different watch lists requiring various forms of action. The No Fly List contained 50,000 persons in 2008 and denies people air transport. The Selectee list contains names of people who are allowed to fly but require more careful searches at airports. The terrorist watch list is the most general and broadest list and may contain anyone that might harm the US. The US terrorist watch list is very controversial for several reasons, not the least for its inclusion of many false positives.
3. United States Attorney Southern District of New York**,** 'Pakistani Man Convicted of Providing Material Support to Al Qaeda Sentenced to 30 Years in Federal Prison,' July 20 2006, http://www.justice.gov/usao/nys/pressreleases/July06/parachasentencingpr.pdf. On proactive prosecution, see Chesney (2005).
4. The US Visitor and Immigrant Status Indicator Technology (USVISIT) programme of border controls integrates and analyses data from diverse sources, including the IDENT biometric database, the APIS passenger manifest database, the Interpol and national crime database IBIS, and CLAIMS3 – holding data on benefits claims, education and health access and finance and banking. Though we cannot be certain that Swift data entered a 'mosaic' of multiple data sources, mined and reassembled, there are precedents such as USVISIT that strongly suggest that in this data war the dots are being connected across plural sources.
5. For instance in the (ongoing) court cases of the assumed Dutch terrorist group de Hofstadgroep, where a key question was *how* to define 'belonging to a criminal group.'

6. Council Decision on the Conclusion of the Agreement between the European Union and the USA on the Processing and Transfer of Financial Messaging Data 2010/0178, Brussels, 24 June 2010, articles 14, 15, 16.
7. Second Report on the Processing of EU-Originating Personal Data by the United States Treasury Department for Counter-Terrorism Purposes, Terrorist Financing Tracking Programme, Judge Jean-Louise Bruguiere, January 2010, EU Classified.
8. Council Decision on the Conclusion of the Agreement between the European Union and the USA on the Processing and Transfer of Financial Messaging Data, 2010/0178, Brussels, 24 June 2010, article 5.3.

REFERENCES

AMERICAN CIVIL LIBERTIES UNION (ACLU). (2009) *Blocking Faith, Freezing Charity: Chilling Muslim Charitable Giving in the 'War on Terrorism Financing'*, ACLU, New York.

AMICELLE, A. (2011) 'The great (data) bank robbery: Terrorist Finance Tracking Program and the "SWIFT affair,"' *Research Questions N°36*, Centre d'études et de recherches internationals, Sciences Po, Paris, May, [Online] Available at: http://www.ceri-sciences-po.org/publica/question/qdr36.pdf (accessed 23 December 2011).

AMOORE, L. (2011) 'Data derivatives: On the emergence of a security risk calculus for our times', *Theory, Culture and Society*, vol. 28, no. 6, pp. 24–43.

AMOORE, L. & DE GOEDE, M. (2008) 'Transactions after 9/11: The banal face of the preemptive strike', *Transactions of the Institute of British Geographers*, vol. 33, no. 2, pp. 173–185.

AMOORE, L. & DE GOEDE, M. (2011) 'Risky geographies: Aid and emnity in Pakistan', *Environment and Planning D: Society and Space*, vol. 29, no. 2, pp. 193–202.

AMOORE, L. & HALL, A. (2009) 'Taking people apart: Digitised dissection and the body at the border', *Environment and Planning D: Society and Space*, vol. 27, no. 3, pp. 444–464.

ANDERSON, B. (2011) 'Population and affective perception: Biopolitics and anticipatory action in US counterinsurgency doctrine', *Antipode*, 43, pp. 205–236.

ARQUILLA, J. & RONFELDT, D. (2001) *Networks and Netwars: The Future of Terror, Crime and Militancy*, RAND, Santa Monica.

BELGIAN PRIVACY COMMISSION. (2006a) *Advies betreffende de doorgifte van persoonsgegevens door de CVBA SWIFT ingevolge de dwangbevelen van de UST (OFAC)*, Advies Nr 37/2006, 27 September 2006.

BELGIAN PRIVACY COMMISSION. (2006b) *Opinion on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas*, opinion No. 37/2006 of 27 September 2006 (non-official translation of the Secretariat of the Commission).

BELGIAN PRIVACY COMMISSION, OR COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LE VENSSFEER. (2008) *Beslissing van 9 december 2008*, [Online] Available at: http://www.privacycommission.be/nl/static/pdf/cbpl-documents/swift—nl-final-09.pdf (accessed 4 June 2010).

CALLON, M. & LATOUR, B. (1981) 'Unscrewing the Big Leviathan: how actors macrostructure reality and how sociologists help them to do so', in *Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies*, eds K.D. Knorr-Cetina & A.V. Cicourel, Routledge/Kegan Paul, Boston, MA, pp. 277–303.

CAMPBELL, D. (2002) 'Time is broken: The return of the past in the response to September 11', *Theory & Event*, vol. 5, no. 4.

CEPS. (2008) *The Impact of New Technologies in the Field of Security: Databases and Biometrics in the EU*, CEPS evening workshop, 25 November.

CHESNEY, R. M. (2005) 'The sleeper scenario: Terrorism support laws and the demands for prevention', *Harvard Journal on Legislation*, vol. 42, pp. 1–89.

COHEN, D. S. (2010) *Remarks to the Washington Institute for Near East Policy*, Washington, [Online] Available at: http://useu.usmission.gov/tftp_040710.html (accessed 23 December 2011).

COUNCIL ON FOREIGN RELATIONS. (2007) *The War on Terrorism: The Financial Front*, Transcript, 10 January, [Online] Available at: http://www.cfr.org/publication/12432/war_on_terrorism.html (accessed 12 October 2010)

COWARD, M. (2009) 'Network-centric violence, critical infrastructure and the urbanization of security', *Security Dialogue*, vol. 40, nos 4–5, pp. 399–418.

DE GOEDE, M. (2012a forthcoming) *Speculative Security: The Politics of Pursuing Terrorist Monies*, University of Minnesota Press, Minneapolis.

DE GOEDE, M. (2012b forthcoming) 'The SWIFT affair and the constitution of a European security community', *Journal of Common Market Studies*.

DE HERT, P. J. A. & DE SCHUTTER, B. (2008) 'International transfers of data in the field of JHA: The lessons of Europol, PNR and Swift', in *Justice, Liberty, Security: New Challenges for EU External Relations*, eds S. Thiel & B. Martenczuk, VUBPress, Brussels, pp. 303–340.

DERDERIAN, J. (2001) *Virtuous War*, Westview Press, Boulder, CO.

ELDEN, S. (2007) 'Terror and territory', *Antipode*, vol. 39, no. 5, pp. 821–845.

ERICSON, R. V. (2007) *Crime in an Insecure World*. Polity, Cambridge.

EUROPOL. (2010) *TE-SAT 2010: EU Terrorism Situation and Trend Report*, Europol, The Hague.

FOUCAULT, M. (2003) *Society Must Be Defended*, tr. D. Macey, Picador, New York.

FOUCAULT, M. (2007) *Security, Territory, Population: Lectures at the Collège de France 1977–1978*, ed. M. Senellart, tr. G. Burchell, Palgrave, Houndmills, Basingstoke.

FRIEDBERG, A. (2007) *The Virtual Window: From Alberti to Microsoft*, MIT Press, Cambridge MA.

GARREAU. (2001) 'Disconnect the dots', *Washington Post*, 17 September, [Online] Available at: http://www.garreau.com/main.cfm?action = chapters&id = 9 (accessed 12 October 2010).

GODINHO, J. (2010) 'When worlds collide: Enforcing United Nations Security Council asset freezes in the EU legal order', *European Law Journal*, vol. 16, no. 1, pp. 67–93.

GONZALEZ FUSTER, G., DE HERT, P. J. A. & GUTWIRTH, S. (2008) 'SWIFT and the vulnerability of transatlantic data transfers', *International Review of Law, Computers & Technology*, vol. 22, no. 1, pp. 191–202.

GRAHAM, S. (2008) 'Imagining urban warfare: Urbanization and US military technoscience' in *War, Citizenship, Territory*, eds D. Cowen & E. Gilbert, Routledge, London, pp. 33–56.

GREGORY, D. (2004) *The Colonial Present: Afghanistan, Palestine and Iraq*, London, Blackwell.

HAGGERTY, K. & ERICSON, R. (2000) 'The surveillant assemblage', *British Journal of Sociology*, vol. 51, pp. 605–622.

HUMAN RIGHTS WATCH. (2004) *The United States 'Disappeared' The CIA's Long Term 'Ghost Detainees'*, [Online] Available at: http://www.hrw.org/legacy/backgrounder/usa/us1004/7.htm (accessed 28 February 2009).

KESSLER, O. & WERNER, W. (2008) 'Extrajudicial killing as risk management', *Security Dialogue*, vol. 39, nos 2/3, pp. 289–308.

KREBS, V. (2002) 'Uncloaking terrorist networks', *First Monday*, vol. 7, no. 4, [Online] Available at: http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/941/863 (accessed 23 December 2011).

KREBS, V. (n.d.) 'Connecting the dots', [Online] Available at: http://orgnet.com/prevent.html (accessed 23 December 2011).

LANGLEY, P. (2008) *The Everyday Life of Global Finance: Saving and Borrowing in Anglo-America*, Oxford University Press, Oxford.

LATOUR, B. (1999) *Pandora's Hope: Essays on the Reality of Science Studies*, Harvard University Press, Cambridge, MA.

LATOUR, B. (2005) *Reassembling the Social*, Oxford University Press, Oxford.

LEVI, M. & GILMORE, B. (2002) 'Terrorist finance, money laundering and the rise and rise of mutual evaluation: A new paradigm for crime control?', *European Journal of Law Reform*, vol. 4, pp. 337–364.

LEVI, M. & WALL, D. S. (2004) 'Technologies, security, and privacy in the post-9/11 European information society', *Journal of Law and Society*, vol. 31, pp. 194–220.

LICHTBLAU, E. (2009) *Bush's Law*, Anchor Books, New York.

LICHTBLAU, E. & RISEN, J. (2006) 'Bank data is sifted by U.S. in secret to block terror', *The New York Times*, 23 June 2006, [Online] Available at: http://www.nytimes.com/2006/06/23/washington/23intel.html (accessed 23 December 2011).

LOS ANGELES TIMES. (2006) 'Secret US program tracks global bank transfers', *Los Angeles Times*, 23 June.

LYON, D. (2003) *Surveillance after September 11*, Polity, London.

MACKENZIE, D. (2005) 'Opening the black boxes of global finance', *Review of International Political Economy*, vol. 12, no. 4, pp. 555–576.

MASSUMI, B. (2005) *Parables for the Virtual*, Duke University Press, Durham, NC, & London.

MEYER, J. & MILLER, G. (2006). U.S. secretly tracks global bank data, *LA Times*, 23 June 2006.

RANSTORP, M. (2007) 'The virtual sanctuary of Al Qaeda and terrorism in the age of globalisation', in *International Relations and Security in the Digital Age*, eds J. Eriksson & G. Giacomello, Routledge, London, pp. 31–56.

REUTERS UK. (2008) 'U.S. terrorism watch list tops 1 million', R. Mikkelsen, 14 July, [Online] Available at: http://uk.reuters.com/article/idUKN1447675120080714 (accessed 23 December 2011).

SAGEMAN, M. (2008) 'The next generation of terror', *Foreign Policy*, March/April, pp. 133–157.

SHAPIRO, M. J. (2009) *Cinematic Geopolitics*, Routledge, London and New York.

SHIELDS, P. (2004) 'When the information revolution and the US security state collide', *New Media and Society*, vol. 7, no. 4, pp. 483–512.

SPARKE, M. (2008) 'Fast capitalism/slow terror: Cushy cosmopolitanism and its extraordinary others', in *Risk and the War on Terror*, eds L. Amoore & M. de Goede, Routledge, London, pp. 133–157.

SULLIVAN, E. (2010) 'Watch lists grows as extra airline screening begins', *Associated Press*, January 4.

SULLIVAN, G. & HAYES, B. (2010) *Blacklisted: Targeted Sanctions, Preemptive Security and Human Rights*, European Center for Constitutional and Human Rights, Berlin.

TAYLOR, J. B. (2007) *Global Financial Warriors: The Untold Story of International Finance in the Post 9/11 World*, W. W. Norton, New York.

US DEPARTMENT OF TREASURY. (2006) *Terrorist Finance Tracking Program Fact Sheet*, 23 June, [Online] Available at: http://www.ustreas.gov/press/releases/js4340.htm (accessed 18 March 2010).

US INSPECTOR GENERAL. (2006) *Survey of US Data Mining Activities*, OIG 06-56, Washington DC.

VAN DER PLOEG, I. (2003) 'Biometrics and privacy: A note on the politics of theorizing technology', *Information, Communication & Society*, vol. 6, no. 1, pp. 85–104.

VLCEK, W. (2008) 'A Leviathan rejuvenated: Surveillance, money laundering, and the war on terror', *International Journal of Politics, Culture, and Society*, vol. 20, pp. 21–40.

WARDE, I. (2007) *The Price of Fear; Al Qaeda and the Truth Behind the Financial War on Terror*, I.B. Tauris, New York.

WASHINGTON POST. (2006a) 'Bank records secretly tapped', 23 June.

WASHINGTON POST. (2006b) 'Officials defend financial searches; Critics assert secret program invades privacy', 24 June.

WILKINSON, P. (2003) *Observations on the New Terrorism*, Foreign Affairs Committee, June, [Online] Available at: http://www.martinfrost.es/htmlfiles/new_terrorism.html (accessed 23 December 2011).

YOUNG, K. DE. (2007) 'Terror database has quadrupled in four years', *Washington Post*, 25 March.

ZARATE, J. C. (2004) 'Bankrupting terrorists', *E-Journal USA*, September, [Online] Available at: http://usinfo.state.gov/journals/ites/0904/ijee/zarate.htm (accessed 19 February 2008)

ZUREIK, E. & SALTER, M. (2005) *Global Surveillance and Policing, Security, Identity*, Willan, Collompton.