Challenge Working Paper

*Work Package 2 – Securitization beyond borders: Exceptionalism inside the EU and impact on policing beyond borders*

# European measures to combat terrorist financing and the tension between liberty and security

September 2005

**Abstract**: This paper discusses recent developments in the campaign to combat terrorist financing in Europe and questions the efficacy of financial surveillance as a method to counter terrorism. A background presentation of surveillance in modern society is followed by an overview of international initiatives to interdict money laundering over the past couple of decades. The measures used to combat terrorist finance are built upon this foundation of surveillance and criminal investigation. Applying these measures in the 'war on terror' has spillover effects for the financial transactions of citizens and non-citizens alike. The paper concludes by considering these problems and their impact on society within the context of a larger concern with liberty as juxtaposed to security in the early 21st century.

William Vlcek
Ph.D. Candidate
Department of International Relations
London School of Economics and Political Science
Houghton Street
London WC2A 2AE
Email: w.b.vlcek@lse.ac.uk

# European measures to combat terrorist financing and the tension between liberty and security*

Nobody expects the Spanish Inquisition!
*– Monty Python's Flying Circus*

The American firm that provided security integration services to the 2004 Athens Olympics employed a friend I have known for a number of years. As a manager in the program control office she was in regular contact with the senior management of the firm, and their counterparts in the Greek Olympic games' organisers. After the conclusion of the games and her vacation to recover from the stress and long hours, she shared via e-mail a number of interesting observations/concerns expressed to her by local Athenians about the surveillance arrangements surrounding the games. 'Weather permitting, the blimp was in Greek airspace throughout both the Olympics and the Paralympics. You know, many of the Greek residents protested the presence of the airship in Athens; they believed that it was monitoring private conversations and that one speaking in his home could be heard and recorded. … But people I met including my neighbors whispered when the airship was nearby and believed it infringed on their right to privacy.'[1]

Individual perceptions of liberty and security are reproduced in the daily lives of ordinary citizens as they submit to the bag inspections and metal detectors that have become ubiquitous upon entry to public buildings, public events and public transportation systems. This paper highlights the more subtle imposition upon personal privacy that emerges from the increased surveillance of our financial transactions that are conducted to prevent the financing of terrorism. This surveillance interrogates the 'normal' financial transactions of citizens and non-citizens. It affects individuals in a variety of ways, to include the opening and maintaining of a bank account, when transferring money between accounts and across borders, when securing a home mortgage, and even when deciding which charity to support.

* This paper was prepared from research conducted for this European Commission funded project on The Changing Landscape of European Liberty and Security, see <www.libertysecurity.org>.

It must be acknowledged that many of the techniques used are not original to the recent effort to combat the financing of terrorism. Rather, they extend global efforts made to counter criminal money laundering first begun decades ago. At the same time, these methods and institutions of surveillance stretch beyond banks and are now embedded within a variety of financial and non-financial business sectors. As Stephen Gill observed,

> much of today's innovation in surveillance practice and technology is driven by state apparatuses—like that of the United States—gathering information about populations and firms, and collecting data on legal and illegal activities for reasons of planning, taxation and control—a process that has intensified in very significant ways since the attacks on the World Trade Center and Pentagon on September 11, 2001. (Gill, 2003: 17)

Gill approaches the issue as but one aspect of disciplinary neoliberalism (Gill, 1995). The global scale of financial surveillance practices has been institutionalised by United Nations Security Council Resolution 1373 (2001). The strategy developed to combat terrorist financing is problematic, however, for three reasons. First is the simple question as to whether or not it has, or is likely to have, any impact upon the conduct of terrorist organisations themselves. Second are the negative consequences these measures have upon the civil liberties of individual citizens. A third reason is a knock-on effect of the second, represented in the impact felt by migrants to the European Union and their ability to remit funds back to their families in foreign states.

The paper is structured in five parts with a general overview of technological surveillance in society presented in the next section. The second section provides background on the international institutions combating criminal money laundering. This includes the Financial Action Task Force (FATF), its various regional progeny (for Europe it is embodied in the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures, MONEYVAL), and the Egmont Group of financial intelligence units (FIUs). The third part outlines the expansion of these organisations/processes from 2001 to explicitly combat the financing of terrorism. The next section describes the situation experienced by citizens as a result of the increased surveillance in banking services (data collection and identity verification) since 2001. The final section summarises this analysis of financial surveillance and the measures to combat terrorist financing in Europe.

**A Surveillance Primer**

In the '10 September 2001' world, surveillance within society was predominately concerned with mundane (non-terrorist) domestic criminal activity. For example, the increased presence of closed-circuit television (CCTV) in public spaces to deter street crime and in retail shops to deter shoplifting. Customers using credit cards were asked to verify identity and signatures were compared in an effort to reduce credit card fraud (Lyon, 2003). Because of the expanding presence of the Internet in the developed states, a concern with computer crime has emerged prompting additional legislation that requires Internet service providers (ISPs) to collect and retain data as an audit trail of citizens' on-line activities. In this 'virtual community' many of the crimes are analogues to those of the physical world (fraud, Ponzi schemes, etc.) and an audit trail of Website connections and e-mail messages can provide the physical evidence necessary for prosecution (Levi and Wall, 2004; Lyon, 2003).

Before 11 September 2001, various attempts to increase and extend surveillance operations to counter the threat of terrorism and other transnational crimes were hindered by the more visible hazard to liberal society and the civil rights of citizens that was presented by increased surveillance. After the terrorist attacks it became an indisputable argument that surveillance was the means that could have prevented/protected against the event. However, the 9/11 Commission found that a number of clues were available to intelligence agencies prior to the attacks, from the surveillance mechanisms then in place (National Commission on Terrorist Attacks upon the United States, 2004). In hindsight, the picture is clear and the clues are obvious, but the point that is relevant to this discussion is the fact that surveillance *already* in place had successfully collected the data. The difficulty was in the collation and analysis of the data, to distinguish signal from noise, and not the result of any absence of relevant data. Increasing the quantity and variety of data will not resolve the problems of collation and analysis, but only reduce the signal to noise ratio and magnify the problem of distinguishing the vital clues present that could be used to prevent any planned terrorist activity.

The structures of observation are manifested in a multitude of subtle ways beyond the electronic trail of one's financial transactions. To be concerned with personal liberty (in the form of privacy) within the bounds of modern society is to worry about a variety of technologies promoted to provide safety and security. There are RFID tags on consumer products, data collection and retention in automobile computing systems, and a prototype for

an 'intelligent' gun (Clothier, 2005).[2] Denis Duclois, in *Le Monde Diplomatique*, took the technologist's dream beyond its limits and crossed a boundary into the territory of the civil libertarian's nightmare when he described the potential to turn vehicle anti-theft features into counter-resistance measures used to subdue critics of the state (Duclos, 2004).[3] The editorial team of *Reason* (a monthly magazine published by the libertarian Reason Foundation to 'promote free minds and free markets') collaborated 'with the direct marketing firm Entremedia, printer maker Xeikon, image provider AirPhotoUSA, and Cal Poly San Luis Obispo, [to utilise] bleeding-edge technologies that allowed [them] to tailor each copy' for the June 2004 issue delivered to their subscribers (Gillespie, 2004). Thus there were more than 40,000 copies of a magazine with specifically localised advertising to demonstrate the 'future of hyperindividualized publications that will be assembled for an audience of one: you' and also to represent the extent to which information about individual citizens are collected and maintained in a variety of databases (Gillespie, 2004). The situation was emphasised by the cover article of the magazine issue, 'Database Nation' and reflects the commodification of personal data in the U.S. marketplace.[4] The European situation is different because of the European Union Data Privacy Directive (Council Directive 95/46/EC). This 1995 directive established a regime of data privacy for EU citizens, including their control over the use of their personal details by private actors (Long and Quek, 2002; Swire and Litan, 1998). This is not to say that such data is not collected and collated on European citizens, only that it has not yet been commodified in the same fashion for commercial business usage. As pointed out by Philippe Bonditti, the collection of data on European citizens (as biometry) has been promoted as a means to provide security (Bonditti, 2004).

These technical capabilities for surveillance serve to provide either security (against crime and terrorism), or efficiency and cost savings (as in the case of RFIDs to track the location of warehouse stock), or safety and convenience (as in the continuing introduction of embedded electronic control systems in vehicles).[5] In general, the populations of the developed states are either unaware of the extent of the surveillance, or simply complicit with the security explanation offered by state authorities. Moreover, authors that are focused on defending society against future terrorist attacks seldom ask normative questions, such as the potential impact to liberal society as a result of their proposal. With the issue of security foremost in their minds (and articles), the presumption made is that the assessment of the need for extensive surveillance is foremost also in the minds of the public. One result of this attitude

is a presumption that security requirements 'trump' other interests in society (in particular personal privacy). Financial surveillance, because the individual account holder observed is explicitly *not* to be informed that police authorities have been provided details on account transactions, is Panoptic in the discrete sense developed by Jeremy Bentham (Bož ovic, 1995). It makes public (to the observing government agents) the private actions of individuals, whilst keeping them explicitly unaware of both the observation and the collection of data. To inform someone that their financial transactions are being monitored is itself a crime.[6] Citizens that are familiar with media discourses involving financial account reporting requirements would know that such observation was possible, but would never know when/if the surveillant eye of the government was focused upon them (Haggerty and Ericson, 2000).

The reaction to any specific proposal to increase surveillance as a counter to terrorism (and previously crime) is a function of cultural context (Welsh and Farrington, 2004: 516; Lyon, 2004: 141 - 143). As Lyon noted, electronic national identity cards are already in use in Southeast Asia (Thailand, Singapore and Malaysia), while the proposals to introduce them in the U.S. and UK are hotly debated.

> In South-East Asia, on the other hand, where more authoritarian and less democratic governments are able to mount systems with little public consultation or approval, it is possible to establish large-scale surveillance systems against a backdrop of much more muted dissent. (Lyon, 2004: 142)

It is this aspect that concerns us about the introduction of increased surveillance with seemly no dissent. The ready acceptance that there is a 'need' for such increased social control returns historical memories of past authoritarian regimes. The specific context for the deployment of any new surveillance system within any individual state may be just as contentious as seen in the UK with the national identity card. There, surveillance cameras are so extensively deployed in major urban areas, public transport and business premises as to be ubiquitous (Webster, 2004: 234 - 235). So ubiquitous is the recognition of the presence of surveillance cameras that there are even contests to identify oneself from the photos published in the newspapers.[7] Yet at the same time, the use of surveillance cameras for traffic control (monitoring for speeding or other illegal conduct) and issuing fines is extremely contentious. The Automobile Association in the UK published a new road atlas for Britain that included the location of highway speed trap cameras, provoking further debate on their use (Bloomfield, 2005). On the other hand, the use of cameras for traffic surveillance and enforcement has been similarly widespread in Germany for many years.

Research investigating the regulation of CCTV and the extent of its usage throughout Europe reached similar conclusions. The United Kingdom has the most extensive CCTV coverage and number of installed cameras in Europe.[8] This situation is the result of measures taken to counter domestic terrorism and the media coverage given the capture of images by a shopping centre CCTV camera showing a young murder victim being abducted by his killers in 1993 (Norris et al., 2004: 111). Similarly, in 1995 the regulatory changes that facilitated an expansion of CCTV in France was in response to worries over increased terrorism (Norris et al., 2004: 122).[9] By contrast, in Germany each Länder regulates the incidence of public CCTV. Marianne Gras found that this circumstance results in essentially three approaches—no legal basis for CCTV in public space, limited authorisation for police surveillance, and those Länder with 'a wider ranging legal permit for police and occasionally other public authorities' to establish a CCTV system (Gras, 2004: 219).

The EU Data Privacy Directive does not serve as complete a shield as we may desire it to serve. Specifically with reference to video surveillance in public space (in shops, pubs and restaurants as well as in streets and train stations) the notification provided by the presence of a sign that a camera is in use suffices as implicit agreement to the capture and preservation of your image. On this point, Gras rightly observes that it does not resolve the question of consent to the surveillance and with the increased prevalence of CCTV throughout public space, our freedom is thereby challenged and potentially reduced. 'If I cannot purchase food without coming under surveillance, how can my consent to that surveillance be said to be free?' (Gras, 2004: 225) Similar to this view is the point made by Jeremy Waldron when developing his argument concerning the image of a balance between liberty and security. He noted that in general the use of 'civil liberties' refers to our diffuse concerns with the power possessed by the state.

> For example, the government's ability to listen in on telephone conversations is a civil liberties concern, even though the 'liberty' in question—sometimes referred to as 'privacy'—does not amount to very much more than the condition of not being subjected to this scrutiny. (Waldron, 2003)

The self-awareness of surveillance, whether by cameras on the street or through the mandated record keeping of the mobile phone company, constrains our freedom of action and our liberty.[10]

Quentin Skinner identified this predicament as a third concept of liberty. When reviewing a new edition of Isaiah Berlin's *Liberty*, Skinner suggested that in addition to positive and negative liberty (as developed by Berlin), there is a third form of liberty. '[T]he essence of the argument is that freedom is restricted by dependence, to be free as a citizen, therefore, requires that the actions of the state should reflect the will of all its citizens, for otherwise the excluded will remain dependent on those whose wills move the state to act.' Consequently for these citizens the 'mere awareness of living in dependence on the goodwill of others serves in itself to restrict our options and thereby limits our liberty.' (Skinner, 2002a)[11] More explicitly, in this context, we live not on the dependence of others, but subject to the unmediated view of the state—all must be seen/audited in order that the few that are engaged in illicit behaviour may be found and removed from the body politic. In essence, we modify our behaviour in the awareness that our financial privacy has become circumscribed by the efforts to prevent terrorism.

**Background – Anti-money Laundering Programmes**

In general, the objective of money laundering is simply to place money into the financial (banking) system in a way that successfully disguises its origins, whether illegal or legal. The illegal source originally targeted for money laundering investigations was the profits from drug trafficking. An example of a legal source would be to place the proceeds of a business transaction into the banking system in order to avoid paying the tax due on any profits. While there is a long history of individuals trying to avoid the confiscatory claims of monarchs, warlords, and highwaymen, one of the earliest contemporary laws involving money laundering may be the U.S. Banking Secrecy Act of 1970. Formally enacted as the Bank Records and Foreign Transactions Act, it did not determine money laundering to be a distinct crime. Rather, it required banks to notify the government of any cash deposits that exceeded $10,000. The objective was to identify potential or probable drug dealers at the point where they would first place their illicit profits into the banking system. The regulatory nature of the law only penalised the bank, for failing to file a currency transaction report, and not the bank customer for the suspected illegal source of their deposit. 'Thus, once the criminal figured out that he could structure his transaction to avoid the $10,000 reporting requirement, the effect of the law on the criminal was only an inconvenience (Adams, 2000: 539)'.

For Europe, the earliest money laundering initiative was a recommendation of the Council of Europe to track the introduction of illegal money entering the banking system (Council of Europe, 1980). The recommendation of the Committee of Ministers to the member states was not, however, directed at drug trafficking. Its objective was to intercept the proceeds of any crimes committed by the left-wing terrorist groups that were plaguing Europe at the time, including the Red Brigades and the Red Army Faction (Pieth, 2002: 365). This particular instrument is more interesting historically as the first instance of a multilateral statement that that the financial sector should take up policing responsibilities against money laundering (Recommendation a). The Council of Europe recommendation was perhaps a little ahead of its time, as the recommendations were not 'widely accepted nor implemented.' (Alldridge, 2003: 96) However, the motivation in 1980 resonates with the declared goals of the more recent initiatives to combat terrorist financing.

Money laundering, as a crime in and of itself, was established in both Britain and the U.S. with the parallel passage of similar legislation in 1986. For the U.S. the strategy to define money laundering as a distinct and independent crime served to establish a second front in the war on drugs. In addition to drug trafficking in the 1986 legislation, Britain would incorporated similar anti-money laundering provisions to anti-terrorism legislation in 1989 in order to combat terrorist financing (Shams, 2004: 28; Alldridge, 2003: 72). The new legislation in the U.S. resolved the problem with the limited enforcement capability of the Bank Secrecy Act (Adams, 2000: 542 - 544). It further brought about a change in the methods of law enforcement agencies because, as a separate criminal charge, it was now separable from the illegal conduct of the original targets – drug traffickers – and could be used against anyone. 'Tacking on a money laundering charge to a crime other than one associated with drug trafficking or organized crime often results in a sentence almost four times what would ordinarily be incurred.' (Adams, 2000: 558 - 559)[12] More recently, the U.S. State Department's 2005 *International Narcotics Control Strategy Report* included a separate volume on 'Money Laundering and Financial Crimes', to emphasise the connection made by U.S. law enforcement between drugs and money laundering. At the same time however, of the sixteen representative law enforcement cases included in the report, only one actually *involved* illegal drugs. The other cases involved various other criminal activities, including fraud, tax evasion, corruption, terrorism and human trafficking (Bureau for International Narcotics and Law Enforcement Affairs, 2005: 12 - 19). In effect, law enforcement authorities are using a charge of money laundering to investigate individuals

whenever there are unexplained financial assets present, even if unable to identify any other substantive (predicate) crime. In the UK this has been codified as 'possessing a criminal lifestyle'. Consequently, if the individual appears to have more income than can be explained via legitimate sources, it must have originated from illegitimate sources. Upon reaching the determination that the defendant had such a 'lifestyle', the court is directed by the legislation to order the confiscation all assets which may have been acquired as a result of criminal activity (Alldridge, 2003: 127 - 129).

The first international convention to direct the criminalisation of any activities involving the 'conversion or transfer of property, … for the purpose of concealing or disguising the illicit origin of the property' was the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (United Nations, 1988: Article 3, paragraph 1(b) (i)). While not using the actual term 'money laundering' the activity described in the convention is nevertheless the same. At the direction of the G-7 Summit held in 1989, the Financial Action Task Force (FATF) was created as part of the international effort to eliminate money laundering associated with drug trafficking. The organisation was described in a more recent communiqué as 'an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. The FATF Secretariat is housed at the OECD.' (Financial Action Task Force, 2005)[13] Towards this end, the FATF has produced evaluation criteria to be used for determining the susceptibility of any firm, agency or national financial system to money laundering activities. With these objectives in mind, the FATF has overseen the development of 'typologies' to describe the methods and techniques used to conceal money laundering. These have been further refined during annual meetings of law enforcement and regulatory experts. These meetings provide a forum to share knowledge on the latest methods attempted to launder money and identified during law enforcement investigations. All of this activity serves to create the basis for the evaluation criteria used to assess compliance with the Forty Recommendations, by member and non-member states alike.[14]

The FATF is at the centre of a 'global network of international organisations and bodies that combat money laundering and terrorist financing' (Financial Action Task Force, 2005). Mark Pieth used the analogy of concentric circles, in which the original members of the FATF lay at the centre in the innermost circle, surrounded by the remainder of the current members of the organisation. Surrounding the FATF circle is the network of regional

affiliate groups (Pieth, 2002: 370). At present these groups include: the Caribbean Financial Action Task Force (CFATF), Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), Asia/Pacific Group on Money Laundering (APG), the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the Financial Action Task Force for South America (GAFISUD), and since late 2004, the Eurasian Group (EAG, which covers China, Russia and several other former Soviet states), and the Middle East and North Africa Financial Action Task Force (MENAFATF). Just as with the FATF, the affiliates promote anti-money laundering policies and facilitate co-operation amongst member jurisdictions to identify and eliminate money laundering and terrorist financing operations.[15]

Within the European Union, the first directive to combat criminal money laundering was approved in 1991 (European Council, 1991). This directive was revised and extended in 2001 (European Parliament and Council of the European Union, 2001), and most recently, the third Directive 'on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing' has been proposed (European Parliament and Council of the European Union, 2004). Alldridge noted that 'there is a clear tension' between the desire of the EU to counter money laundering as a threat to the economy and the capacity of the EU, as a governmental entity, to implement and enforce criminal laws against money launderers (Alldridge, 2003: 97). Notwithstanding this difficulty, these EU Directives take on-board the FATF recommendations, and extend their influence beyond the domestic legislation of member states. Those neighbouring states that have ratified the European Economic Area (EEA) agreement are obligated also to incorporate the money laundering directive into their domestic law (Gilmore, 2004: 195). The activities of the FATF and other agencies to identify the evolving techniques used to launder money served to highlight deficiencies in the 1991 EU Directive as written. During the mid-to-late 1990s attempts to revise and promulgate a new EU money laundering were hampered by two significant points of contention. The first point of concern was the move to broaden the coverage of the anti-money laundering directive to include additional predicate crimes. This revision would be in keeping with changes made to the FATF Forty Recommendations in 1996 (Gilmore, 2004: 202).[16]

The second area of concern was the move to extend the range of surveillance coverage beyond financial institutions. The objective here was to expand the awareness and reporting

obligations to those professions and firms that could facilitate money laundering outside of the banking business sector. Included within the scope of this expansion were lawyers, accountants, tax advisors, insurance firms, jewellers, and casinos. It was a controversial expansion that raised a question about the infringement of lawyer/client confidentiality (Alldridge, 2003: 100; Gilmore, 2004: 202). The debates surrounding these two points hindered the adoption of the second money laundering directive for over three years. Ultimately, it took the 11 September 2001 attacks to surmount the stand-off, as they intensified the argument that 'controls upon international terrorism required more effective control of money laundering' (Alldridge, 2003: 100). Approval of the Second Money Laundering Directive was but one of the measures taken to increase the capability of states to legally pursue those that finance terrorism, the next section discusses some of these other measures.

**Extension – to Combat Terrorist Financing**

The techniques and strategies used to counter money laundering were quickly extended and applied against the financing of terrorism following the events of September 2001. The FATF expanded the scope of its financial system oversight and analysis to include the financing of terrorist activities. In an 'extraordinary' session held on 29 - 30 October 2001 in Washington, D.C., the FATF broadened its mandate, and agreed to eight special recommendations that would serve as 'new international standards for combating terrorist financing' (Financial Action Task Force, 2003a: 1). At issue was the use of funds originating from both legitimate and illegitimate sources to finance terrorist activities. The first of these additional recommendations, however, simply calls for the ratification and implementation of 'UN instruments', specifically the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism and United Nations Security Council Resolution 1373 (2001). The remaining seven recommendations encourage states to:

- criminalise the financing of terrorism, terrorist acts and terrorist organisations, and to designate these activities as predicate offences for money laundering;
- institute measures to freeze the funds and assets of terrorists, terrorist financiers and terrorist organisations;
- establish reporting mechanisms for any suspicious financial transactions related to terrorism;

- promote international legal co-operation related to these efforts to combat the financing of terrorism;
- license informal/alternative financial networks and subject them to the FATF recommendations on money laundering and terrorist financing;
- require all wire transfers to include 'accurate and meaningful originator information';
- insure that non-profit organisations 'cannot be misused' for the financing of terrorism (Financial Action Task Force, 2001).

With regard to these *Special Recommendations on Terrorist Financing*, Jean-Marc Sorel observed that they 'restate rather than innovate the most relevant measures expressed previously in the framework of terrorism.' (Sorel, 2003: 373) The real difficulty, as some FATF member jurisdictions reported, was 'that terrorist financing might not meet the definition of money laundering [which] meant that they were limited in the actions they could take against terrorist monies in the framework of anti-money laundering laws.' (Financial Action Task Force, 2002: 2) This problem was recognised by the UN team tasked to monitor compliance with UN Security Council Resolution 1373 (2001).[17] Consequently, the Counter-Terrorism Committee (CTC) has been co-ordinating technical assistance, especially with drafting new legislation, to help non-compliant UN member states to meet the requirements of the resolution (Ward, 2003).

The public reaction to the terrorist attack gave state authorities the opportunity to include those businesses that they had previously been unable or unwilling to force into the campaign against money laundering. This change is reflected in both the USA PATRIOT Act revisions to U.S. banking and anti-money laundering laws, and the approval of the second EU Money Laundering Directive (Council Directive 2001/97/EC).[18] The explicit inclusion of various non-financial services business activities and individuals has now conscripted a wide range of firms into the fight against both money laundering and the financing of terrorism. This change was universalised in the revision to the FATF Forty Recommendations in 2003. The previous version had suggested that 'appropriate national authorities should consider applying' the Recommendations to any *financial* transactions a non-financial services firm might perform. Characterised as 'designated non-financial businesses and professions', these firms were now explicitly identified as possible avenues for money laundering activity. Amongst the named non-financial firms are casinos, realtors, lawyers, accountants, jewellers, and trust and company service providers. Thus, while they are not 'financial' businesses,

they all potentially handle sizeable quantities of money. With the 2003 version of the FATF document, Recommendation 20 now encourages the application of the Recommendations to any other businesses and professions 'that pose a money laundering or terrorist financing risk' (Financial Action Task Force, 2003b: 7; Financial Action Task Force, n.d.).[19]

The sheer magnitude of the task now facing the financial services industry and government agencies to monitor financial transactions must be recognised. Every significant transaction (either suspicious in itself or in excess of US$10,000/€15,000) is to be subjected to review and analysis (FATF Recommendation 13). The 1995 report of the Office of Technology Assessment provided figures of 700,000 wire transfers a day within the United States, totalling in excess of $2 trillion ('of which perhaps from 0.05 percent to 0.1 percent represent money laundering'). (U.S. Congress Office of Technology Assessment, 1995: 9)[20] In 2000, a magazine article noted that the U.S. Financial Crimes Enforcement Network (FinCEN) received over 12 million Currency Transaction Reports (CTRs, submitted for a cash transaction over $10,000) and an average of 10,000 Suspicious Activity Reports (SARs) a month from banks (Wakefield, 2000). Even though reporting requirements are now extended to cover check cashing services, investment/brokerage firms, lawyers, accountants, insurance companies, etc., the number of CTRs reported for fiscal year 2002 was still only 12.8 million (Financial Crimes Enforcement Network, 2002: 2). In 2002, the number of SARs was 281,373, significantly increasing to 507,217 reports for 2003 and subsequently to 689,414 reports in 2004 (Financial Crimes Enforcement Network, 2005). For comparison, in the UK the National Criminal Intelligence Service (NCIS) reported that in the period 2002 - 2003 the number of SARs received was 'about 60% greater than in 2001 - 2002.' (National Criminal Intelligence Service, 2003: 11)[21] Just as academics and researchers find themselves overwhelmed by the sheer mass of information available, so too are financial analysts, bank staff, and regulatory and crime enforcement agencies. The increasing number of reported transactions only serves to further bury and conceal any suspicious transactions actually indicative of money laundering or terrorist financing.

> Fraud experts such as Liesel Annible of accountants Bentley Jennison, who is UK president of the Association of Certified Fraud Examiners, believes the system can actually help criminals.

> "What does NCIS do with all these reports? Firms are now disclosing so much because of the fear of prosecution that there is a danger of serious infringements being hidden by and lost under all the noise of all the minor problems and unfounded suspicions. All these SARs just gum up the works - the vast majority are just stored," she says. (Levene, 2003)

In the process of trying to cover all possible avenues available to launder money, governments have massively increased the analysis workload facing law enforcement agencies.

**The Lived Experience – Banking since 2001**

Probably the most common, and frequent, encounter with the expanded financial surveillance regime since 2001 is a request for multiple forms of identification. This information has become necessary in order to open an account, establish a new/different account with the same institution, make a deposit, purchase a home or insurance policy, to exchange foreign currency or to wire money. The customer experience is universal in that it is recommended by the FATF (Recommendation 5) and required by the EU Money Laundering Directive (Article 3). The requirement for a bank to 'Know Your Customer' (KYC) is not only a problem for those that explicitly desire to conceal their finances from state authorities (and in so doing avoid the original intention for the law). It is also problematic for those existing on the fringes of society within developed states, including migrant labour, recent immigrants, and the homeless. These individuals are not in a position to engage with formal banking structures (due to the cost to establish and maintain an account as much as the requirements for documentation), and as a result they may use an informal banking system (hawala, hundi, fei ch'ien, etc.), especially to send money home to family and friends. While in the case of migratory labour and emigrants these transactions are individually small, the aggregate quantities remitted to their home states may be substantial and a significant economic factor for the receiving states (World Bank, 2003; World Bank, 2004).

Since the passage of the 2003 Money Laundering Act in the United Kingdom, the emphasis on Know Your Customer (KYC) has at times appeared to go overboard. Problems with the inconsistent implementation of the requirement in the UK banking industry are recognised by regulatory officials. The Financial Services Authority official responsible for financial crime matters spoke about 'Anti-money laundering regulation - next generation developments' to the City & Financial Conference in 2004. He provided a couple of anecdotal examples while

emphasising the important contribution of the identification requirement to prevent money laundering.

> There can be a funny side to this, such as the Oxford College required to produce its 15th century charter, complete with seal in order to open a new account. More often, it just seems mindlessly irritating, as it seemed for the senior colleague of mine trying to open an account for his daughter at a branch, only to be told (wrongly) that a council tax bill is not a utility bill! (Robinson, 2004)

Recognising that both the banking industry and banking customers have been inconvenienced by the increased emphasis on customer identification, the FSA undertook a programme to 'defuse the issue'. They have involved a variety of interested parties in a working group to build a common understanding of the issues and assist in determining methods to improve the process of establishing customer identification in the financial services sector (Financial Crime Sector, 2004).

For the established, employed citizen, the experience with providing identification at the bank is very often simply an annoyance, whereas for others the demand for multiple forms of identification and proof of local (permanent) residence may be an insurmountable obstacle to financial services. As de Goede has noted, the use of risk classification as a method to identify suspicious individuals in the campaign against terrorist financing may result in their financial exclusion. The effect of this methodology is to segregate from the general population individuals without regular financial transactions or a fixed address. In addition to suspected terrorists, this segregated group would include migrant workers, students and the unemployed. Essentially anyone that could also fit the risk profile of being a *potential* terrorist (de Goede, 2005: 38; see also de Goede, 2004: 9). The absence of suitable documentation, and the cost of maintaining a bank account, means that participation in the formal banking system is difficult for this stratum of society. This is not to suggest that the industry is unaware of the problem of financial exclusion. In a speech to the Financial Services Authority Conference on Fraud and Money Laundering in 2004, the Chief Executive of the British Bankers' Association outlined the organisation's participation in work to address the issue. One of these activities was 'an extensive consultative exercise with voluntary organisations, banks, regulators and others to lengthen the "long list" of appropriate [identification] documents for people who are financially excluded.' He went on to highlight, as a sign of success in this area, the establishment of 800,000 new 'basic bank accounts'

through a cooperative programme between the government and the banking industry to reduce the number of financially excluded (Mullen, 2004).

Combining the difficulties experienced to establish a formal bank account with the cultural experience of immigrant workers in the use of informal (traditional) banking practices promotes the continued use of these informal systems.[22] This system of informal banking has existed for centuries and relies upon 'ethnic-based trust' and it is a desire to avoid social sanctions in the ethnic community rather than formal legal structures that maintains the integrity of the system (Masciandaro, 2004: 267). Consequently, the emphasis is upon the trust relationship and not upon the source or destination of the funds transferred by this informal financial intermediary (hawaladar).

> According to the [Malaysian] money changers they are not overly concerned about the source of the money being sent. What is important is that the person on behalf of whom the money is being sent be known to the money changer. (Shanmugam, 2004: 43)

Because of the informal, undocumented (and thus unauditable) nature of informal banking systems, they are not only used for migrant worker remittances home to some remote village in India, Pakistan, the Philippines, or Mexico, but they have been used also to avoid taxes and capital controls. The undocumented nature of informal systems immediately mark them out as suspicious because they may be used to facilitate money laundering and terrorist financing (Financial Action Task Force, 2000; Financial Action Task Force, 2004). The U.S. government acted upon these suspicions when it shut down the informal Somali banking enterprise known as 'al-Barakaat' (de Goede, 2003; Ruehsen, 2002a; Ruehsen, 2002b).

The FATF had already identified informal banking as a method for money laundering in 1999 and now for terrorist financing (Financial Action Task Force, 1999: 10). The recommended solution is to *formalise* the informal (Special Recommendation on Terrorist Financing VI). This means for example that the Malaysian Anti-Money Laundering Act of 2001 requires money changers to keep records, formally identify customers and report suspicious transactions to the Financial Intelligence Unit of the Malaysian Central Bank (Shanmugam, 2004: 42). Forcing the informal system to operate more like the formal system increases the cost of doing business, and corrodes the trust relationship on which these systems are grounded. As pointed out above, cost and the lack of formal documentation for identification were reasons for using the informal money transfer system. In pursuit of the few potential

wrongdoers, the many, once again, have great difficulty in transferring money home to family and friends. As already noted above, the aggregate amount of migrant remittances is quite substantial. In 2002, *reported* remittances to developing countries amounted to US$88.1 billion, vastly exceeding official development assistance (World Bank, 2004: 169). The estimate for 2003 projected these *reported* remittances as increasing to US$93.0 billion.[23] For individual states, these remittances can be vital to domestic growth. The Philippines for example receives between 9 and 10 percent of its GDP in the form of remittances from overseas Filipino workers (OFW) (Guerrero, 2005). In 2004 that was US$ 8.55 billion in total, with US$ 1.27 billion identified as originating from Europe. The Central Bank of the Philippines qualifies the data with two notes. First, it is limited to those funds transferred through the formal banking system and second, the designated country of origin is taken from the immediate source of the transfer.

> Data are not truly reflective of the actual country of deployment of OFW's due to the common practice of remittance centers in various cities abroad to course remittances through correspondent banks mostly located in the U.S. Since banks attribute the origin of funds to the most immediate source, U.S., therefore appears to be the main source of OFW remittances. (Central Bank of the Philippines, 2005b)[24]

A survey conducted of overseas Filipinos over the period 1995 - 2002 asked them which remittance channel they used, and formal banks accounted for 69 per cent (Guerrero, 2005). This situation will change in the future as the informal banking structures of the Philippines were required to register with the Central Bank from 24 January 2005 (Central Bank of the Philippines, 2005a).

The important point is that constraining the informal banking system has the potential of a far more detrimental impact upon developing states than it has for any likelihood to identify and isolate terrorists. In a study of 'Migration and Illegal Finance' Donato Masciandaro considered the case of Italy and attempted to answer the question—'what relationship exists between the phenomenon of migrations and the risk of financing terrorism?' (Masciandaro, 2004: 268 - 271) The conclusion Masciandaro reached, based on an aggregate analysis of the available empirical data, was that the data did not support 'the existence of a relationship between the risk of financing Islamic terrorism and the intensification of migration [remittance] flows'. (Masciandaro, 2004: 271) Moreover, Charles Calomiris observed that if Osama bin Laden 'can recruit 30 people willing to die on his behalf, he will have no problem

getting 100 to open bank accounts.' (Tsingou, 2005: 101-102, citing *The Economist*, 29 September 2001)[25] The implication is that technological solutions using risk analysis methods and comparing customer transaction patterns against those of the notional terrorist sympathiser may be easily circumvented by mundane methods using the large pool of supporters attracted to the declared goals of a terrorist organisation. An extended group of ordinary citizens could be quietly recruited to provide very simple support—adding to their 'normal' pattern of financial transactions, for example, a small monthly transfer to another account, using cash provided to them anonymously.

To counter these simple solutions requires better human intelligence on terrorist organisations and not terabytes of data recording the financial transactions of the population at large. Yet financial institutions, faced with the legislated demands that they interdict the financing of terrorism, may choose to take a more basic approach to risk reduction. In addition to the various hurdles presented by a bank (in order to comply with anti-money laundering and terrorist financing regulation) discussed above, the individual account holder could be confronted with simple discrimination. Tsingou made this point when she described the problem created when this policing responsibility was placed upon banks and other financial institutions. Essentially, banks are now expected to make a value judgement about customers and their money and whether they may be involved in some terrorist activity, *in the future.*

> … this is a subjective and time-consuming strategy that can also lead to discrimination on the basis of ethnic background and create biases linked to personal characteristics. (Tsingou, 2005: 101)

There have already been cases that appear to reflect this assessment. For example, there was the decision by the Royal Bank of Scotland to close the long-standing accounts it held on behalf of a Palestinian charitable group, Friends of Al-Aqsa, and of its chair, Ismail Patel. At the same time, the Alliance and Leicester bank closed the account of the Palestine Solidarity Campaign (al Yafai, 2005).[26]

**Conclusions – Financial security at what cost to liberty/privacy?**

The bottom-line is – to what extent do you value privacy (from your neighbours as much as from the state) and how much are you willing to exchange for security? A number of authors declare that this image of a balance is a false dichotomy, including security expert Bruce Schneier who insisted that security and liberty 'are not two sides of a teeter-totter.'

(Schneier, 2003: 250) It is a question then of risk assessment and the response to this question and assessment of risk is very individualistic. Yet the solution established by the state is not geared towards permitting *individual* assessments of risk, but rather weighted to benefit law enforcement and intelligence gathering agencies. As an example, consider the insistence on inspecting the shoes of airline passengers by the Transportation Security Administration (TSA) in the U.S. This exercise is a reaction to the failed attempt by one lone individual to ignite a quantity of explosives he had concealed in his shoes. The policy statement provided on the TSA website reads,

> You are NOT REQUIRED to remove your shoes before you enter the walk-through metal detector. However, TSA screeners may encourage you to remove them before entering the metal detector as many types of footwear will require additional screening even if the metal detector DOES NOT alarm. (Transportation Security Administration, 2005, emphasis in original)

This situation highlights another point made by Schneier, that the fundamental rationale for judicial and legislative restraints upon law enforcement officials in a democratic society is to prevent the abuse of power. 'These constraints have been created not to make the police ineffective, but because people know that the inevitable police abuses would be worse were the laws not in place.' (Schneier, 2003: 67 - 68) The loss of these restraints, as much as the loss of liberty, is the tragic consequence for society, and a demonstration that success is possible from terrorist action. When the purpose of terrorism is to create fear amongst a target population, than the reaction demonstrated by the various surveillance and security measures mentioned in this paper indicate the success of the terrorist attacks.[27] The fear generated by the 11 September 2001 attacks facilitated acquiescence that allowed the enactment of legislative measures that had been previously obstructed for their illiberal nature. Subsequent attacks in Madrid and London have motivated European leaders to similarly enact more stringent measures against terrorism.

The conceptualisation of a balance between liberty and security further highlights the question of whose liberty? This has been analysed by Didier Bigo for the Hague Programme's application of the term 'freedom'. Here, Bigo argues that there are 'at least 67 ways to conceptualises the relations' that exist between freedom, security, justice and danger. Crucially, the 'balance' that may be achieved amongst these relations 'depends on the hierarchy of values a community shares.' (Bigo, 2005) This observations explains why the focus placed on the danger originating from footwear by U.S. airport security is not found at a European airport, the hierarchy of concerns between the security systems are different.

Furthermore, it explains the long-standing observation made prior to September 2001 about the frailty of American airport security against hijacking, as compared to Europe and, at the extreme, Israel.

By contrast, financial institutions now are held responsible to identify and report suspicious activity, and if their anti-money laundering/terrorist financing system is evaluated and found lacking, they are subject to penalties. Domestically that means the institution is fined, for example, in 2003, the Abbey National Bank was fined £2,320,000 and the Northern Bank was fined £1,250,000 for failures to comply with existing anti-money laundering regulations (Harvey, 2004: 338). Internationally, that means that domestic institutions will be blocked from executing transactions with the banned foreign institution, for example two banks in Latvia identified by FinCen as 'primary money laundering concerns'. Acting under the provisions of the USA PATRIOT Act this declaration by the U.S. government requires U.S. financial institutions to take 'certain "special measures" against the designee.' (U.S. Treasury, 2005) Just the announcement by itself had an immediate effect on the named banks according to a Latvian news report (The Baltic Times, 2005).

The surveillance of financial transactions as part of the effort to combat terrorist financing does not actually address the risk of terrorism itself. It does, however, significantly expand the capacity of the state to reproduce a 'data double' for any of its residents. The surveillant assemblage creates a vast collection of data about residents and visitors (Haggerty and Ericson, 2000). From within this monumental stack of straw and hay the state security services attempt to isolate and remove the violent few that seek to wreak havoc and create fear in society. The danger to democratic society is that this expanded police power is not limited simply to the pursuit of terrorism. One analysis of the EU's Common Position on the application of specific measures to combat terrorism emphasised the point that there was a limited intellectual debate to define 'terrorism' for it.[28] The political solution that resulted from this compromise definition carries with it the potential to establish as 'terrorist' a variety of actions that previously would not have been considered acts of terrorism but merely political dissent.

> If terrorism is to encompass hackers and organizations that protest in the North Sea then – to put it somewhat bluntly – the efforts to fight money laundering become part of the problem as well. They are at risk of being perceived as instruments of repression and terror. (Pieth, 2002: 376)

The solution offered by the Common Position suggests the existence of a separate law enforcement agenda with respect to computer crime and environmental activism, and as a result it was this agenda that found its way into the EU's Common Position.[29] However, should this agenda come to reflect a more common perception, it may initiate a move back towards the original reason, and justification, for banking secrecy. The rationale (*ex post facto* perhaps) offered by Switzerland for the maintenance of banking secrecy was the historical experience of German Jews before World War II (Faith, 1982: 49 - 87). If any resistance to government policy may be categorised and treated as 'terrorist', political dissent in a democratic society may disappear, and residents pursue avenues to conceal their financial transactions.

The point raised about financial exclusion due to the processes of financial surveillance to combat terrorist financing resonates with a wider concerned raised before 2001 about surveillance in general (Lyon, 2001). In this context financial exclusion is simply one facet of the wider problem of social exclusion created by the use of surveillance in society. These 'anonymous' or 'indiscriminate' modes of surveillance foster and promote social exclusion, and as such have the potential for technologically-based forms of discrimination and, if you will, segregation in society between those that are clearly 'okay' and those that for one reason or another are 'suspicious' and therefore must be kept separate, identified, and known (Lyon, 2003). Waldron arrived at a similar conclusion in his assessment of the balance between liberty and security, one that intersects with Bigo's question concerning whose liberty is at risk. 'We should be even more careful about giving up our commitment to the civil liberties of a minority, so that we can enjoy *our* liberties in greater security.' (Waldron, 2003: 210, emphasis in the original) Fundamentally, privacy, as a right *not* to be subjected to surveillance (to be free of surveillance and the hazard of an omnipresent eye of the sovereign), is thus a 'civil liberty'. Consequently, in the face of a terrorist threat this civil liberty has come to be represented as negotiable, if not completely null and void, in order to achieve security.

More recent experience with CCTV in London, following the attacks of July 2005, underscores the dilemma with using this method of surveillance to counter terrorism. Captured and retained images serve well as an audit trail of events and as evidence for judicial proceedings. As a defensive measure, however, the presence of cameras will not *prevent* the determined attack, and in some circumstances serves only to displace criminal

activity to un-surveilled locales (Welsh and Farrington, 2004: 502), or to force behaviour changes, such as wearing hooded coats and hats as a means of concealment from the ubiquitous camera. Financial surveillance achieves similar results, providing an audit trail and legal evidence as well as displacing activity, in this case through informal value transfer networks or bulk cash smuggling.

The answer to the overarching question—does financial surveillance interdict the financing of terrorism—is quite simple, we don't know. Recall that one difficulty with criminalising terrorist financing is that the funds could be completely ordinary and innocuous until they have been *used* for terrorism. Freezing the accounts of *known* terrorists and terrorist organisations does not tackle the *unknown* accounts of supporters containing the moneys that will be used for the next to-be-determined attack. This risk is the great challenge for the campaign to combat terrorist financing, in Europe as elsewhere.

Word count: 12,219

**Endnotes**

[1] What is just as interesting as these anecdotes in themselves is how they were offered with the implicit suggestion that the Athenians had misunderstood or misconstrued the purpose and capabilities of the security apparatus, and the simple fact that *citizens* had nothing to fear from it. Yet, given the Greek experience with military government and an antiterrorist security regime, their concerns and conclusions are understandable.

[2] RFID is the acronym for Radio Frequency IDentification—a technology that has become more prominent in recent years because of the increasingly small package size possible. See (Granneman, 2003).

[3] This potential capability was portrayed via special effects in the film *After the Sunset* (2004) when at the very beginning the criminals established remote control of a police vehicle in order to commit their theft.

[4] It is a situation that is also reflected in an e-mail circulating around the Internet since at least January 2004, when this author first received 'Ordering Pizza in 2015'. In this piece of Internet humour, the pizza company knows an extensive amount of information about a

customer, available from their national identification number. This includes not only where they live, but also the status of their bank account, credit card account, and health (they refuse to sell him a pizza that is inappropriate for his blood pressure and cholesterol level).

[5] With regard to these automotive systems, and in particular the ability to monitor the driving activities of one's teenage children, see for example (Higgins, 2005).

[6] For a discussion of 'tipping-off', see (Alldridge, 2003: 200ff)

[7] See for example the *Lite Standard* (London) 'Is this you?' contest.

[8] For further analysis of CCTV in Britain see (Mccahill and Norris, 2002).

[9] Eurobarometer polls subsequent to the U.S. terrorist attacks in 2001 reflect an increased concern with terrorism, which we may take to mean an increased acceptance of anti-terrorism measures. The 2002 report highlighted citizens' growing anxieties, where '86% of Europeans say that they personally fear terrorism (12 percentage points more than one year earlier)' (Directorate-General Press and Communication, 2002: i)

[10] My line of thought here on liberty and security is indebted to a short article that forced me to question my previous understanding of liberty and the notional balance between liberty and security. See (Aradau, 2005)

[11] There is a more detailed development of this argument for a third concept of liberty in (Skinner, 2002b).

[12] This law journal article discussed U.S. laws and this remark is specific to the Federal sentencing guidelines in place at the time.

[13] The members of the FATF, as of 11 February 2005, are: Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, China, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, Kingdom of the Netherlands, New Zealand, Norway, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States. Additional members represent the European Commission and the Gulf Co-operation Council, and effective on this date, China was accorded observer status.

[14] Initially released in 1990, the Forty Recommendations document was revised in 1996 to account for the first six years of experience formally combating money laundering. There was then a major revision in 2003 to incorporate the measures recommended to combat the financing of terrorism.

[15] See the FATF website <http://www.fatf-gafi.org/>.

[16] The change in question involved the conversion of Recommendations 4 and 5 of the 1990 version into Recommendation 4 of the 1996 (which was then rolled-up into Recommendation 1 of the 2003 revision). The 1990 text was explicitly linked to illegal drugs, whereas the 1996 text reads 'Each country should extend the offence of drug money laundering to one based on serious offences. Each country would determine which serious crimes would be designated as money laundering predicate offences.'

[17] See < http://www.un.org/Docs/sc/committees/1373/>

[18] The USA PATRIOT Act was a hodgepodge of law enforcement measures that had been set aside in the past after determining they were contrary to American ideals of liberty, freedom, and civil rights. Michael Levi reported that 'my interviews indicate that following widespread opposition justified on the grounds of privacy concerns and organized by an e-mail lobby of bankers (in unusual collaboration with left- and right-wing privacy enthusiasts) to Congress and the media, these proposals were withdrawn in 2000 until terrorism reoriented privacy values in 2001.' (Levi, 2002: 187)

[19] From the obvious to the sublime in the methods used to finance terrorism. One of the men arrested in connection with the 11 March 2004 Madrid bombings was a dealer in counterfeit designer clothing. The conclusion reached as a result was that the global market for counterfeit luxury goods is financing terrorism. The secretary general of Interpol was quoted as saying in an address to the U.S. Congress, 'Intellectual property crime is becoming the preferred method of funding for a number of terrorist groups.' The NCIS in Britain did not agree with this position, replying to the information request of a journalist with the statement –

> Claims that there are links between other sectors of serious crime and IPC [intellectual property crime] are not substantiated by available intelligence. Paramilitary groups active in Northern Ireland use IPC to support criminal terrorist activity but there is no intelligence to support other links between IPC in the UK and terrorist activity. (Eagar, 2005)

[20] This amounts to between $1 and $2 million a day of *suspected* money laundering.

[21] The NCIS website reported – 'In 2003, NCIS received around 100,000 disclosures - an increase of nearly 60 per cent on 2002, itself nearly double 2001's figures.' (National Criminal Intelligence Service, 2005)

[22] Traditional informal banking systems in the Middle East and Asia are variously known as 'hawala', 'hundi', 'fei ch'ien', 'phoe kuan', 'hui k'nan', 'ch'iao hui', and 'nging sing kek'. See (Shanmugam, 2004)

[23] The *Global Development Finance* (2004) Appendix on remittances was quite clear that the figures reported only those funds that passed through formal banking systems. While the increases in reported remittances from 2001 to 2003 may represent in part an increased use of formal banking (as a result of the increased regulation of informal transfer agents), nonetheless a large portion of total remittances continue to move via informal banking systems. 'Officials in major fund-transfer agencies argue, based on the volume of funds flowing through their systems, that unrecorded remittances may be larger than recorded remittances.' (World Bank, 2004: 170)

[24] This situation was also found by Roger Ballard to be true for UK-base hawaladars who aggregated their local funds and transferred them to Dubai-based Exchange Houses on accounts maintained at New York City banks (in U.S. dollars) (Ballard, 2003: 10 - 12).

[25] Calomiris is the Henry Kaufman Professor of Financial Institutions at Columbia University.

[26] These actions in the UK follow earlier American action taken against charities. The Texas-based Holy Land Foundation was closed in 2001. The Palestinian charity was accused of providing funds to Hamas, a U.S.-designated terrorist organisation (FT.com staff, 2001).

[27] The definition deployed by Schneier was 'Terrorism is not a movement or ideology, but a military tactic. A terrorist is someone who employs physical or psychological violence against noncombatants in an attempt to coerce, control, or simply change a political situation by causing terror in the general populace.' (Schneier, 2003: 69)

[28] Council Common Position 2001/931/CFSP on the application of specific measures to combat terrorism OJ 2001 L 344/93

[29] Recent events in Denmark would appear to justify this concern for a broad application of these anti-terrorist measures. Greenpeace Nordic was charged and convicted as the responsible organisation behind the activity of a group of activists. In October 2003, these activists staged a protest denouncing GMO food at the headquarters of the Danish Agriculture Council. The organisation had been charged under laws passed to implement UN and EU directives to combat terrorist financing. As noted by the defence lawyer in remarks to Statewatch—'I think that a lot of the politicians now feel that this is an

unpleasant case and that this use of the amendment was not what they intended.' (Statewatch, 2005) See also (Formisano, 2005).

**References**


ADAMS, T. E. (2000) Tacking on Money Laundering Charges to White Collar Crimes: What did Congress intend, and what are the courts doing? *Georgia State University Law Review*, 17, no. 2: 531 - 573.

AL YAFAI, F. (2005) Palestinian aid groups' accounts closed. *The Guardian* (London) 3 January.

ALLDRIDGE, P. (2003) *Money Laundering Law: Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime.* Oxford, Hart Publishing.

ARADAU, C. (2005) *The Other Hobbesian State*. Challenge. Accessed 20 July 2005, last revised 19 April, available at <http://libertysecurity.org/article213.html>.

BALLARD, R. (2003) *Hawala Transformed: Remittance-driven Transnational Networks in the post-Imperial economic order*. Manchester, Centre for Applied South Asian Studies, University of Manchester, available at <http://www.art.man.ac.uk/CASAS/pdfpapers/transformed.pdf>.

BIGO, D. (2005) *Liberty, whose liberty? The Hague Programme and the conception of freedom*. Challenge. Accessed 20 July 2005, last revised 20 July, available at <http://libertysecurity.org/article339.html>.

BLOOMFIELD, S. (2005) AA Causes Fury by Publishing its First-ever Map of Speed Cameras. *Independent on Sunday* (London) 26 June. sec. News: 8.

BONDITTI, P. (2004) From Territorial Space to Networks: A Foucaldian Approach to the Implementation of Biometry. *Alternatives*, 29, no. 4: 465 - 482.

BOŽOVIC, M. (Ed.) (1995) *Jeremy Bentham: The Panopticon Writings*, London, Verso.

BUREAU FOR INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS (2005) *International Narcotics Control Strategy Report, Volume II - Money Laundering and Financial Crimes*. U.S. Department of State. Accessed 12 March 2005, last revised March, available at <http://www.state.gov/g/inl/rls/nrcrpt/2005/>.

CENTRAL BANK OF THE PHILIPPINES (2005a) Circular No. 471.

—— (2005b) *Overseas Filipino Workers' Remittances By Country and By Type of Worker*. Accessed 10 June 2005, last revised 3 June, available at <http://www.bsp.gov.ph/statistics/sefi/ofw.htm>.

CLOTHIER, J. (2005) *Fighting crime with smart firearm*. CNN.com. Accessed 4 February 2005, last revised 31 January, available at <http://edition.cnn.com/2005/TECH/01/31/spark.intelligent.firearm/index.html>.

COUNCIL OF EUROPE (1980) *Measures Against the Transfer and Safekeeping of Funds of Criminal Origin: Recommendation and Explanatory Memorandum*. Rec(80)10E, last revised 27 June.

DE GOEDE, M. (2003) Hawala discourse and the war on terrorist finance. *Environment and Planning D*, 21: 513 - 532.

—— (2004) *The Risk of Terrorist Financing: Politics and Prediction in the War on Terrorist Finance*. Constructing World Orders Conference, The Hague, last revised 9 - 11 September.

—— (2005) Risk and the war on terrorist finance. *Operational Risk*, March, 36 - 41.

DIRECTORATE-GENERAL PRESS AND COMMUNICATION (2002) *Eurobarometer: Public Opinion in the European Union*. Brussels, European Union, last revised April, available at <http://europa.eu.int/comm/public_opinion>.

DUCLOS, D. (2004) Watching them watching us. *Le Monde diplomatique*, September, 12 - 13.
EAGAR, C. (2005) *Fake London*. Evening Standard, London, last revised 11 February.
EUROPEAN COUNCIL (1991) *Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.* Official Journal of the European Communities (hereinafter OJ) L series 166, last revised 28 June.
EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION (2001) *Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.* Official Journal of the European Communities (hereinafter OJ) L series 244, last revised 28 December.
—— (2004) *Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing.* COM (2004) 448 final, last revised 30 June.
FAITH, N. (1982) *Safety in Numbers: The Mysterious World of Swiss Banking.* London, Hamish Hamilton.
FINANCIAL ACTION TASK FORCE (1999) *Report on Money Laundering Typologies, 1998 - 1999.* English ed. Accessed 21 March 2002, last revised 3 February, available at <www.oecd.org/fatf/pdf/TY2000_en.pdf>.
—— (2000) *Report on Money Laundering Typologies, 1999 - 2000.* English ed. Accessed 21 March 2002, last revised 3 February, available at <www.oecd.org/fatf/pdf/TY2000_en.pdf>.
—— (2001) *Special Recommendations on Terrorist Financing.* English ed., Paris. Accessed 24 September 2002, last revised 31 October, available at <http://www1.oecd.org/fatf/pdf/SRecTF_en.pdf>.
—— (2002) *Report on Money Laundering Typologies, 2000 - 2001.* English ed. Accessed 21 March 2002, available at <www.oecd.org/fatf/pdf/TY2001_en.pdf>.
—— (2003a) *Annual Report 2001 - 2002.* English ed. Accessed 1 July 2002, last revised 21 June, available at <http://www.fatf-gafi.org/dataoecd/13/1/34328160.pdf>.
—— (2003b) *The Forty Recommendations (2003).* English ed., Paris. Accessed 30 June 2003, last revised 20 June 2003, available at <http://www.fatf-gafi.org/dataoecd/38/47/34030579.PDF>.
—— (2004) *Report on Money Laundering and Terrorist Financing Typologies, 2003 - 2004.* English ed. Accessed 1 September 2004, available at <http://www.fatf-gafi.org/pdf/TY2004_en.PDF>.
—— (2005) *FATF Welcomes China as an Observer*. Accessed 18 February 2005, last revised 11 February, available at <http://www.fatf-gafi.org/dataoecd/51/2/34423127.pdf>.
—— (n.d.) *The Forty Recommendations.* English ed., Paris. Accessed 6 February 2002, available at <http://www1.oecd.org/fatf/pdf/40Rec_en.pdf>.
FINANCIAL CRIME SECTOR (2004) *ID - defusing the issue: A progress report*. Financial Services Authority, last revised October, available at <http://www.fsa.gov.uk/pubs/other/id_report.pdf [accessed 8 June 2005]>.
FINANCIAL CRIMES ENFORCEMENT NETWORK (2002) *Use of Currency Transaction Reports*. Washington, D.C., U.S. Department of the Treasury, last revised October, available at <http://www.fincen.gov/section366report.pdf [accessed 25 January 2004]>.
—— (2005) *The SAR Activity Review: By the Numbers*. Washington, D.C., U.S. Department of the Treasury, last revised May, available at <http://www.fincen.gov/sarreviewmay2005.pdf [accessed 9 June 2005]>.
FORMISANO, M. (2005) *Is Greenpeace a terrorist organisation under EU law?* , Challenge. Accessed 4 July 2005, last revised 14 June, available at <http://www.libertysecurity.org/article283.html>.

FOUCAULT, M. (1995) *Discipline & Punish: The Birth of the Prison*. Second Vintage ed. New York, Vintage Books.
—— (2003) *"Society Must Be Defended" Lectures at the Collège de France, 1975 - 1976*. New York, Picador.
FT.COM STAFF (2001) *US closes down charity with alleged Hamas links*. Special Reports - Attack on Terrorism ed., FT.com. Accessed 8 March 2005, last revised 14 February 2002, available at <http://specials.ft.com/attackonterrorism/FT3BYVCYTUC.html>.
GILL, S. (1995) Globalisation, Market Civilisation, and Disciplinary Neoliberalism. *Millennium: Journal of International Studies*, 24, no. 3: 399 - 423.
------ (2003) American Transparency Capitalism and Human Security: A Contradiction in Terms? *Global Change, Peace and Security*, 15, no. 1: 9 - 25.
GILLESPIE, N. (2004) Editor's Note: Kiss Privacy Goodbye -- and Good Riddance, Too. *Reason*, June, 2?
GILMORE, W. C. (2004) *Dirty Money: The evolution of international measures to counter money laundering and the financing of terrorism*. Third ed. Strasbourg, Council of Europe Publishing.
GRANNEMAN, S. (2003) *RFID Chips Are Here*. SecurityFocus.com. Accessed 30 March 2005, last revised 27 June, available at <http://www.theregister.co.uk/2003/06/27/rfid_chips_are_here/>.
GRAS, M. L. (2004) The Legal Regulation of CCTV in Europe. *Surveillance & Society*, 2, no. 2/3: 216 - 229.
GUERRERO, R. (2005) *Statistical Measurement of Overseas Filipino Workers' Remittances: Present Practices and Future Direction*. A Presentation to the International Technical Meeting on Measuring Migrant Remittances, Central Bank of the Philippines. Accessed 28 March 2005, last revised 25 January, available at <http://www.worldbank.org/data/Remittances/4dGuerrero.ppt>.
HAGGERTY , K. D. & ERICSON, R. V. (2000) The surveillant assemblage. *British Journal of Sociology*, 51, no. 4: 605 - 622.
HARVEY, J. (2004) Compliance and Reporting Issues Arising for Financial Institutions from Money Laundering Regulations: A Preliminary Cost Benefit Study. *Journal of Money Laundering Control*, 7, no. 4: 333 - 346.
HIGGINS, M. (2005) Big Brother Now Rides With Teen Drivers. *Wall Street Journal Europe* (Brussels) 24 February. sec. Networking: A7.
LEVENE, T. (2003) Why rules won't wash on money laundering. *The Guardian* (London) 28 June. sec. Jobs and Money.
LEVI, M. (2002) Money laundering and its regulation. *Annals of the American Academy of Political and Social Science*, no. 582: 181 - 194.
LEVI, M. & WALL, D. S. (2004) Technologies, Security, and Privacy in the Post-9/11 European Information Society. *Journal of Law and Society*, 31, no. 2: 194 - 220.
LONG, W. J. & QUEK, M. P. (2002) Personal data privacy protection in an age of globalization: the US - EU safe harbor compromise. *Journal of European Public Policy*, 9, no. 3: 325 - 344.
LYON, D. (2001) *Surveillance society: Monitoring everyday life*. Buckingham, Open University Press.
—— (2003) *Surveillance after September 11*. Cambridge, Polity.
—— (2004) Globalizing Surveillance: Comparative and Sociological Perspectives. *International Sociology*, 19, no. 2: 135 - 149.
MASCIANDARO, D. (2004) Migration and Illegal Finance. *Journal of Money Laundering Control*, 7, no. 3: 264 - 271.
MCCAHILL, M. & NORRIS, C. (2002) *CCTV in Britain*. Urbaneye Working Paper No. 3, last revised March, available at <www.urbaneye.net>.

MULLEN, I. (2004) *Anti-money laundering - An industry view*. British Bankers' Association. Accessed 28 March 2005, last revised 26 October, available at <http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=222&a=4620>.

NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004) *The 9/11 Commission Report.* Washington, D.C., National Commission on Terrorist Attacks upon the United States.

NATIONAL CRIMINAL INTELLIGENCE SERVICE (2003) *Annual Report and Accounts: A year in the fight against serious and organised crime 2002 - 2003*. London, available at <www.ncis.gov.uk>.

—— (2005) *Financial intelligence*. Accessed 8 June 2005, available at <http://www.ncis.co.uk/financialintelligence.asp>.

NORRIS, C., MCCAHILL, M. & WOOD, D. (2004) The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance & Society*, 2, no. 2/3: 110 - 135.

PIETH, M. (2002) Financing of Terrorism: Following the Money. *European Journal of Law Reform*, 4, no. 2: 365 - 376.

ROBINSON, P. (2004) *Anti-money laundering regulation - next generation developments.* Accessed 8 June 2005, last revised 21 April, available at <http://www.fsa.gov.uk/Pages/Library/Communication/Speeches/2004/SP180.shtml>.

RUEHSEN, M. (2002a) Fallacy of Sanctions. *Middle East Insight*, 17, no. 2: 31 - 34.

—— (2002b) Tracing Al-Qaeda's Money. *Middle East Insight*, 17, no. 1: 41 - 44.

SCHNEIER, B. (2003) *Beyond Fear: Thinking Sensibly About Security in an Uncertain World.* New York, Copernicus Books.

SHAMS, H. (2004) *Legal Globalization: Money Laundering Law and Other Cases.* London, British Institute of International and Comparative Law.

SHANMUGAM, B. (2004) Hawala and Money Laundering: A Malaysian Perspective. *Journal of Money Laundering Control*, 8, no. 1: 37 - 47.

SKINNER, Q. (2002a) A Third Concept of Liberty. *London Review of Books*, 4 April, 16 - 18.

—— (2002b) A Third Concept of Liberty. *Proceedings of the British Academy*, 117: 237 - 268.

SOREL, J.-M. (2003) Some Questions About the Definition of Terrorism and the Fight Against Its Financing. *European Journal of International Law*, 14, no. 2: 365 - 378.

STATEWATCH (2005) *Greenpeace charged under anti-terror laws.* Statewatch News Online. Accessed 4 July 2005, last revised June 2005, available at <http://www.statewatch.org/news/2005/may/04greenpeace.htm>.

SWIRE, P. P. & LITAN, R. E. (1998) *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive.* Washington, D.C., Brookings Institution Press.

THE BALTIC TIMES (2005) *U.S. government blacklists two Latvian banks.* Realty.lv. Accessed 19 September 2005, last revised 28 April, available at <http://www.realty.lv/eng/news/?category=&id=383960280420051131 32>.

TRANSPORTATION SECURITY ADMINISTRATION (2005) *Travelers & Consumers: Prepare For Takeoff.* Accessed 7 June 2005, available at <http://www.tsa.gov/public/interapp/editorial/editorial_1049.xml>.

TSINGOU, E. (2005) Targeting Money Laundering: Global Approach or Diffusion of Authority? In KRAHMANN, E. (Ed.) *New Threats and New Actors in International Security.* Houndmills, Basingstoke, Palgrave Macmillan.

U.S. CONGRESS OFFICE OF TECHNOLOGY ASSESSMENT (1995) *Information Technologies for Control of Money Laundering.* Washington, D.C., U.S. Government Printing Office.

U.S. TREASURY (2005) *Treasury Wields PATRIOT Act Powers to Isolate Two Latvian Banks Financial Institutions Identified as "Primary Money Laundering Concerns.* JS-2401 ed., Office of Public

Affairs. Accessed 19 September 2005, last revised 21 April, available at <http://www.treas.gov/press/releases/js2401.htm>.
UNITED NATIONS (1988) *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention).*
WAKEFIELD, J. (2000) *Following the Money*. Government Executive Magazine. Accessed 10 May 2002, last revised 1 October, available at <http://www.govexec.com/features/1000/1000s5.htm>.
WALDRON, J. (2003) Security and Liberty: The Image of Balance. *Journal of Political Philosophy*, 11, no. 2: 191 - 210.
WARD, C. A. (2003) Building Capacity to Combat International Terrorism: The Role of the United Nations Security Council. *Journal of Conflict & Security Law*, 8, no. 2: 289 - 305.
WEBSTER, W. R. (2004) The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK. *Surveillance & Society*, 2, no. 2/3: 230 - 250.
WELSH, B. C. & FARRINGTON, D. P. (2004) Surveillance for Crime Prevention in Public Space: Results and Policy Choices in Britain and America. *Criminology & Public Policy*, 3, no. 3: 497 - 526.
WORLD BANK (2003) *Global Development Finance: Striving for Stability in Development Finance.* Washington, D.C., IBRD/World Bank.
—— (2004) *Global Development Finance: Harnessing Cyclical Gains for Development.* Washington, D.C., IBRD/World Bank.