PRIVACY AS ROGUERY: PERSONAL FINANCIAL INFORMATION IN AN AGE OF TRANSPARENCY

J.C. SHARMAN

A fundamental shift has occurred in the relationship between the state and the individual regarding financial privacy. The onus is now on citizens to show why governments should not have access to their personal financial information, rather than governments having to show why they should. This article argues that this shift has come about in large part because of the activities of autonomous and influential transnational networks of regulators. These regulatory networks have systematically favoured administrative efficiency and transparency at the expense of privacy in designing responses to financial crimes. Evidence is drawn from an examination of recent policy developments in countering tax evasion, money laundering, and the financing of terrorism. Currently, the principle of financial transparency suggests that financial privacy inhibits the fight against criminals and terrorists; by extension, asserting a right to privacy indicates some kind of roguery afoot.

People’s banking and other financial information comprise an intimate portrait of their lives. Yet the currently dominant principle of financial transparency holds that individual citizens have no legitimate reason to keep their personal financial data private from the state. Expressing the now conventional view, a senior international policy-maker in this area has asserted: ‘Where secrecy lies, roguery is not far behind’. In relation to financial information the usual presumption of privacy has been reversed: the onus is increasingly on citizens to provide a good reason why their personal information should remain private, rather than the authorities having to provide a good reason to gain access. Evidence to support this contention is drawn from an examination of recent policy developments in the fight against tax evasion, money laundering, and the financing of terrorism.

The core of this new regulation has been formulated within and diffused through networks of regulators working as part of international organizations, particularly the Organization for Economic Co-operation and Development (OECD) and the Financial Action Task Force (FATF). These transnational networks of like-minded experts and technocrats, in setting international standards, privilege administrative efficiency and bureaucratic rationality (Slaughter 2004; Barnett and Finnemore 2004). Privacy concerns have had little effect in restricting increased state access to personal financial information because these closed transnational networks of regulators have enjoyed considerable latitude in designing new standards to achieve functional policy goals. The change is in part the result of a contest of principles (Braithwaite and Drahos 2000). It has been successfully argued that the need for free and unfettered access to personal financial data in order to combat criminals and terrorists supersedes the principle of a right to privacy. Conversely, this view holds, asserting a right to privacy creates restrictions on the state’s access to this information, which aids criminals and terrorists, and as such is \textit{prima facie} evidence of roguery of one kind or another. Somewhat ironically, the principle...
of transparency, introduced with an eye to making governments more open to citizens, has been employed to the reverse effect in making citizens more open to governments.

The result is that in nearly all OECD countries, a wide range of government officials can order that personal financial information be turned over by banks and other private firms, while these firms face civil or criminal prosecution if they inform customers that their data have been disclosed in this way. New regulations require financial intermediaries to collect, store and distribute personal data in line with ‘Know Your Customer’ procedures. Through ‘Suspicious Transaction Reporting’ requirements, law enforcement bodies maintain huge databases of electronic financial transfers. Because cash is a largely anonymous medium of exchange compared with electronic transactions, recent rules limit its use. Administrative procedures have come to replace judicial safeguards in the exchange of personal financial data between agencies within one country, as well as in cross-border exchanges (FATF 2004, 2007a; OECD 2006, 2007).

In order to make an argument about how conceptions of financial privacy have changed, it is first necessary to spell out what financial privacy is, and why it might be important. The next task is to sketch the nature of transnational regulatory networks in explaining how they can possess both autonomy and influence over the international standard-setting process. The intertwined imperatives of administrative efficiency, specialization, and delegation have long been known to empower bureaucracies in relation to their erstwhile masters, but this dynamic is often under-appreciated at the transnational level. The three sections that follow provide evidence for the contention that these networks have effected a diminution of financial privacy. It does this by detailing recent policy developments in three related fields: the efforts to counter tax evasion; money laundering; and the finance of terrorism. In all three areas the policy problem at issue has been successfully characterized as a problem of information, with transparency presented as the solution, and privacy as an obstacle to policy success.

WHAT IS FINANCIAL PRIVACY AND WHY IS IT IMPORTANT?

Before examining the importance of transnational networks and particular policy developments, it is important to settle on some working definitions. Bennett and Raab note that ‘It is an almost ritual feature of any analysis of privacy . . . to begin with a warning about the inherent difficulty, perhaps impossibility, of defining exactly what “privacy” is’ (Bennett and Raab 2006, p. 6). As a response they decline to provide any such definition. These difficulties notwithstanding, for the purposes of this article, privacy is defined as ‘the claim of an individual to determine what information about himself or herself should be known to others’ (Westin 2003, p. 431). The advantage of Westin’s definition is that it is a good fit with the everyday understanding of this concept (Bennett and Raab 2006, pp. 14–19). Once socially or legally recognized, privacy claims become rights (Westin 2003, p. 431), in this case ‘the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed’ (Westin 1967, p. 42). There are competing philosophical views on what the right to privacy is or should be (Cohen 2002; Nagel 2002; Palm 2007), but, given the empirical, policy focus of this piece, these debates are left to one side. This article takes right in a deontological sense, that is, people have inalienable rights ‘just because’ (Margulis 2003). There may also be utilitarian, social arguments for preserving financial privacy (Regan 1995). Some have pointed out the tendency of corrupt governments or particular officials to misuse financial data collected by the state (Hay 2001). But these
concerns are secondary. A right to privacy is enshrined in some important human rights
documents, including the European Convention on Human Rights Article 8, and the
Charter of Fundamental Rights Articles 7 and 8. The Fourth Amendment to the US
constitution also sets out certain privacy rights.

Like other rights, the right to privacy is not absolute. Just as free speech does not
extend to defamation, inciting crime or shouting ‘fire’ in a crowded theatre, so too it
is uncontroversial that privacy can be compromised to defend other rights or social
interests. An absolute right to privacy would, for example, make any modern tax system
unworkable, with all the attendant consequences for the provision of public goods.
However, like free speech, the presumption is, or rather has been, that the onus is on
governments to provide a compelling reason why privacy should be compromised, rather
than the onus being on citizens to show why privacy should be upheld.

Working from this basis, financial privacy is simply taken as the right of an individual
to determine what financial information about themselves should be known to others.
Although the ‘others’ in question may refer to other private individuals or firms, for
current purposes, it is the capacity of an individual to control what personal financial
information is known to the state that is at issue. Why might financial privacy be important
in practical terms? Existing literature on privacy has devoted relatively little attention
to the contest for control over personal financial information between citizens and the
state, as opposed to that between consumers and private firms (Bennett and Raab 2006).
People’s financial data provide an important picture of who they are. Most obviously,
such information reveals whether people are rich or poor. In OECD economies it usually
also reveals where people work and the nature of their occupation. However, with the rise
of electronic forms of payment, especially credit and debit cards, financial information
gives a much more detailed portrait. In the United States, a majority of transactions
are now carried out with credit cards (of which the average household has ten) (see ‘A
Cash Call’, Economist 15 February 2007). Credit cards (or debit cards) are somewhat less
common in other OECD countries, but the trend is towards increased use. In addition,
from a low base, electronic means of payment are also rapidly expanding in developing
countries. Because (unlike cash) electronic payments link a particular person with a
particular purchase, it is possible to follow patterns of consumption, as well as often
tracking a person’s movements. For private firms, people’s spending patterns comprise
valuable information precisely because on this basis it is possible to extrapolate a great
deal about the individual in question.

Revealing a person’s financial details can have far-reaching consequences. In some
 cultural contexts, wealth is stigmatized, in others poverty can lead to social exclusion.
Thus individuals who are significantly richer or poorer than their peers may wish to
keep this fact private. Financial transactions can reveal a person’s health, marital status,
lifestyle, hobbies and much more. Indeed, some commentators argue that in the context of
a consumer society, identities are primarily formed and expressed through consumption
(Bourdieu 1984). Transactions may reveal the purchase of goods and services that may be
shunned even when they are legal (for example, pornography or prostitution; talk-show
host Jerry Springer’s forced resignation from the Cincinnati local government after paying
for a prostitute with a personal cheque standing as a cautionary tale). Financial data could
expose behaviour that falls into the same category: maintenance to an unacknowledged
child; adultery; or the relative warmth of feelings towards different family members
expressed in a will. In general, for most people in rich Western countries, the list of
an individual’s financial transactions would probably be far more revealing than, for
example, the list of phone numbers called or received, or the contents of letters sent and delivered.

TRANSNATIONAL NETWORKS AND THE CONTEST OF PRINCIPLES

The literature thus far has tended to see threats to privacy as coming from either individual states (keen on instituting the ‘surveillance society’, see Gandy 1993; Lyon 2001), or multinational firms. In contrast, international organizations and transnational networks of regulators and technocrats tend to be presented in a positive light. For example, Bennett and Raab speak of the importance of the transnational network of privacy and data protection officials. They note the steps taken by the OECD, Council of Europe, International Standards Organization and EU to safeguard privacy (Chapter 4). Even the World Trade Organization explicitly protects governments’ prerogatives to regulate trade so as to protect privacy (2006, p. 88). However, in contrast to this positive treatment, it is argued here that such transnational networks and international organizations have recently played a vital role in reversing the presumption in favour of financial privacy. Two bodies in particular have taken the lead in this context: the OECD’s Committee on Fiscal Affairs on tax, and the Financial Action Task Force (FATF) on money laundering. The FATF and the OECD have been able to capitalize on but also advance a principle of financial transparency that has come to eclipse financial privacy. This section argues that such transnational policy networks enjoy considerable autonomy from national democratic control. They exercise a great deal of influence over setting international standards, which are subsequently transposed into national legislation.

The tendency of specialized bureaucracies to usurp democratic control in the name of administrative efficiency has been known for at least a century. Thus Robert Michels wrote of how the mass base of social democratic parties lost control as the efficient functioning of the organization required delegation to a bureaucratic oligarchy (1911). Drawing on the work of Michels and especially Max Weber, Barnett and Finnemore (1999, 2004) characterize international organizations as stereotypical bureaucracies. Bureaucracies exercise authority through the creation of impersonal rules and in the rational, technocratic and ostensibly apolitical manner in which they go about their business (Barnett and Finnemore 2004, p. 3). These authors criticize the tendency to see international organizations as passive tools of states, and instead contend that the ‘rational-legal authority that IOs [International Organizations] embody gives them power independent of the states that created them and channels that power in particular directions’ (1999, p. 699). Rather than just being informational clearing-houses, international institutions sift, sort and interpret information to create new classifications, categories, rules and actors. A related series of edited volumes provides more than two-dozen detailed case studies in support of this rendering (Reinalda and Verbeek 1998; Reinalda and Verbeek 2004; Joachim et al. 2008).

Networks of regulators situated in international organizations, particularly the FATF and the OECD, have been central in the design and diffusion of new measures to stop tax evasion, money laundering and the financing of terrorism. Why have these networks had such an impact, and why have they acted to privilege administrative efficiency over other concerns, particularly financial privacy? Writing with particular reference to the FATF and OECD, Anne-Marie Slaughter (2004) sees transnational networks of regulators as essential for responding to cross-border threats, and as epitomizing the new, disaggregated state. Such networks achieve influence through their expertise, control over information, and
ability to socialize members who exercise the domestic legal authority that such networks themselves lack. The FATF itself has no legal standing, and nor do its 40 Recommendations on countering money laundering and 9 Special Recommendations on terrorist financing. Yet having gained acceptance amongst those attending FATF plenaries, conducting Mutual Evaluation Reports and writing interpretive guidance notes, these individuals then go home to translate the recommendations into hard law (Levi and Gilmore 2002).

Although the OECD is a formal treaty organization, the vast majority of its output (including that of the Committee on Fiscal Affairs on tax) is again informal recommendations, model conventions, guides to best practice, and so on (Marcussen 2001, p. 4; Porter and Webb 2004, p. 5). Once again, these informal guidelines then form the basis for a great deal of hard law, for example, the large majority of double tax treaties (which are designed to protect against the risk of an individual or corporation being taxed twice where the same income is taxable in two jurisdictions). Despite being part of a larger organization, the composition of the Committee on Fiscal Affairs is highly congruent with the FATF: a like-minded group of mid-level national officials with a common functional specialization interacting with each other and the secretariat in pursuit of technical knowledge and administrative efficiency (Sharman 2006, pp. 72–3). As Marcussen relates, the OECD’s mode of influence over national policy processes is also similar to that of the FATF: ‘National civil servants develop a common selective perception of the world and they start to employ a common frame of reference and a common worldview. The latter helps them to define what can be considered as a relevant problem in the first place and which instruments can legitimately be employed to solve this problem’ (2001, p. 21; see also Porter and Webb 2004, p. 10).

Slaughter sees such networks as being particularly effective precisely because they are relatively small, selective groups of similarly situated individuals with common training and professional socialization. Rather than getting side-tracked by diplomatic niceties and political posturing, networks concentrate on solving practical problems as efficiently as possible. Because this work is generally expressed in esoteric, technical language, and carried out behind closed doors, there is little need to worry about spin or public relations in translating the network consensus into policy. No ministers or journalists attend FATF plenaries, and the FATF has no mechanism to consult either the private sector or non-governmental organizations. Of the hundreds of pages of documents presented at FATF meetings, only a tiny fraction are ever made public. Similarly, the OECD Committee on Fiscal Affairs is comprised of a permanent secretariat and a rotating cast of mid-level national tax officials working in various sub-committees and working groups. On the rare occasions that ministers are briefed on these activities, they rarely read the briefs (Interviews with OECD officials). Members of national legislatures have no involvement. Tax information exchange agreements are not the stuff of headlines or demonstrations. For the relevant transnational policy networks, the increasing preference for administrative rather than judicial arrangements in collecting and exchanging personal financial data both domestically and internationally is again explained on the basis of efficiency. Slaughter thus come to essentially the same conclusion as Barnett and Finnemore regarding the autonomy and influence of bodies such as the OECD and FATF, though the latter are far less sanguine than Slaughter concerning the implications for democracy, or even policy effectiveness.

As Barnett and Finnemore relate, international organizations gain much of their authority from the imperative to achieve generally valorized goals in an efficient manner. In their encyclopaedic study, Global Business Regulation, Braithwaite and Drahos identify
‘contests of principles’ over such goals as crucial to the globalization of regulation (2000, Chapter 21). Principles simplify the incredible complexity faced by regulators by giving succinct, stylized prompts to action: for example, the principle of most-favoured nation in trade policy or best available technology in environmental regulation. Of all those examined in the book, ‘transparency is the most striking emergent principle of globalization’ (2000, p. 508). This principle has become closely associated with fighting corruption thanks to the international NGO Transparency International and, more broadly, with making governments more open and accountable to citizens. But the resonance of transparency as a principle has now been appropriated and reversed by governments in order to make the financial affairs of firms, associations and individuals transparent. As demonstrated below, this principle has now been realized in the policy and regulatory changes affecting tax, anti-money laundering and terrorist financing.

In driving and justifying this change, international organizations and governments have argued that barriers to obtaining access to personal financial data make it difficult to pursue policy goals that enjoy widespread popular support, such as reducing crime and terrorism. These same parties also maintain that a right to privacy works to the benefit of criminals and terrorists. Empirically, both statements are very probably true. Furthermore, these policy developments appeal to a commonsense logic that says: ‘If you aren’t doing anything wrong, you shouldn’t be concerned about your privacy; if you are doing something wrong, then it is all to the good that we know about it’. Hence also the quote at the beginning of this article from the OECD Committee on Fiscal Affairs official paraphrasing Samuel Johnson on privacy and roguery. Perhaps convincing on its own terms, the logical application of the argument that a given right hinders governmental efficiency and effectiveness, and benefits miscreants, would, however, lead to the suspension or abolition of most checks on state power.

TAX EVASION

Historically, the practices of tax evasion (breaking the law to escape tax obligations) and tax avoidance (minimizing one’s obligations within the law) have shaped societies in ways large and small. In modern times, the result of this struggle has hinged more than any other factor on the ability of governments to gather information about wealth and income, and natural and legal persons’ ability to deny governments this information (Slemrod 2006). With the growing relevance of cross-border economic linkages, the pursuit of information by governments has increasingly required co-operation and co-ordination between states.

The OECD has been central in the process of both documenting and encouraging the international exchange of tax information. OECD publications are valuable summaries of the state of play in tax information collection (see, for example, OECD 2006). But the organization has a further important standard-setting role in the area of access to and international exchange of tax information. Although the membership is limited to 30 rich countries, OECD regulatory standards often come to comprise the global benchmark (Braithwaite and Drahos 2000, p. 29; Porter and Webb 2004). Thus, while the United Nations and the OECD both have templates for international tax information exchange as part of their respective model double tax treaties, it is the OECD example that has diffused much more widely (Interview with UN Tax Committee). The OECD has sought to assist the efforts of tax collectors in gathering financial information in related efforts to promote financial transparency within and beyond its membership.
The most relevant project, ‘Increasing Access to Bank Information for Tax Collection Purposes’, is hosted by the OECD Committee on Fiscal Affairs (OECD 2000, 2003, 2007). The ‘ideal standard’ sought by the initiative is that ‘all Member countries should permit access to bank information, directly or indirectly, for all tax purposes so that tax authorities can fully discharge their revenue raising responsibilities and engage in effective exchange of information with treaty partners’ (OECD 2000, p. 3). From the OECD’s point of view, the ideal policy standard in this area is most closely represented by Australia.

In Australia, the tax authorities, working in conjunction with the anti-money laundering authority, can compel banks to hand over all financial data on their customers. No justification has to be provided. This process is administrative rather than judicial, so there is no need either for a warrant or recourse to the court system. Banks must not inform their customers that their financial data has been requested or handed over, on pain of being held civilly and criminally liable for prosecution. These powers are in addition to the routine obligation of banks to automatically pass on information about interest payments, and the more than 15 million financial transaction reports passed on to the Financial Intelligence Unit annually (Austrac 2007, pp. 34–7; see also explanation below in connection with money laundering).

As part of the OECD’s work on fiscal transparency, certain practices are especially discouraged as creating obstacles to tax collection. Prominent amongst these is banking secrecy (OECD 2000, 2001, 2003, 2006). Bank secrecy refers to laws that make bank employees criminally liable for revealing an account holder’s information to any third party, including the host or foreign government. The earliest prominent example was a federal law passed in Switzerland in January 1934, subsequently copied by other small states looking to establish offshore financial centres (Palan 2003). In Austria, prior to 2000, passbook savings accounts were known only by a number, so that whoever held the physical account book owned the account, there was simply no name entered. Even when government access to bank account details is not completely prohibited in jurisdictions with strong bank secrecy, securing this information usually involved going through a tortuous and long-winded series of legal manoeuvres vulnerable to appeals by the bank on a variety of grounds. Account holders so targeted had years of notice to close the accounts and move their money elsewhere.

In order to streamline this process, over the last decade the OECD has consistently sought to encourage member and non-member countries to allow governments to get hold of and exchange financial information for tax purposes on an administrative basis, bypassing the courts (OECD 2000, 2003, 2007). The rationale is that the relevant information can be secured much more quickly and cheaply, without the chance that the authorities will have their request disallowed. Additional consequences are that there is no independent check that regulates government access to financial information, and no chance for the individual or firm to contest the government’s right to access the data.

At the international level, the preference for administrative rather than judicial procedure is reflected in the OECD’s drive for tax information exchange agreements, either on a stand-alone basis, or as part of double tax treaties (OECD 2006). These exchange agreements are designed to prevent tax payers evading their tax obligations at home by hiding their money offshore. Reflecting privacy concerns, these agreements previously prevented ‘fishing expeditions’. An example of a fishing expedition might be if tax authorities in the United States asked their counterparts in the Bahamas to hand over all financial information on citizens of the United States with Bahamian bank accounts. Instead, to be legitimate, requests must relate to a specific individual’s account.
at a specific financial institution in a situation where that individual is already under investigation. But the wording of the 2004 OECD model exchange agreement indicates that this prohibition on fishing expeditions has now in effect been relaxed. Tax authorities, unsurprisingly, regard protecting revenue as more important than protecting privacy, a shared mentality that is reinforced by personal links mediated through the OECD and other tax bodies (the Commonwealth Association of Tax Assessors, Inter-American Centre for Tax Administration, International Fiscal Studies Association, International Taxation Dialogue, UN Committee of Experts on International Co-operation on Tax Matters, and so on).

Apart from the bar on fishing expeditions, there were two other important limitations to the international exchange of information which are now no longer regarded as legitimate (OECD 2004, 2007). The first is the criterion of fiscal interest, the second double criminality. Fiscal interest means that the country fielding the foreign request (for example, the Bahamas) must stand to gain some tax revenue by providing information to the foreign country (for example, the United States). The logic behind this has been that gathering information is costly, and that no sovereign country has a duty to act as tax collector for any other foreign jurisdiction. Currently, however, under both OECD and UN model tax treaties, countries are expected to provide information to foreign tax authorities even in the absence of a direct fiscal interest, both as a ‘mark of good international citizenship’ (G20 2004, p. 1), and on the assumption that over the longer term exchanges will result in a roughly equal distribution of benefits (OECD 2007, p. 6). The second limitation was the requirement of dual criminality: the act in question must constitute a crime in the foreign jurisdiction as well as the country lodging the request. For example, since Switzerland does not regard tax evasion as a criminal offence, it refuses to hand over information to foreign tax evasion investigations. With the (major) exceptions of Switzerland and Luxembourg, all OECD countries have now dropped the dual criminality requirement for tax crimes (OECD 2007, p. 4), as have tax haven countries which themselves do not levy any income taxes (OECD 2006).

Governments have discovered a further source of tax-related information in successfully pressing non-bank financial intermediaries to hand over otherwise confidential data useful for tax collection purposes. In particular, this dynamic is observable in the tendency to take the credit card companies VISA and MasterCard to court to force them to release card holders’ financial data. A tactic first employed by the US government in March 2002, it has since been successfully copied by the UK and Australia. Credit and debit cards have been a common means to repatriate money held offshore for the purposes of evading taxes at home. The US government took VISA and MasterCard to court to obtain the records of all US residents who had credit or debit cards issued by financial institutions in specified countries alleged to be tax havens. By this means the US obtained records on 230,000 individuals (Sharman and Rawlings 2006). The British and Australian government followed suit in obtaining records on their own residents with offshore credit and debit cards, gaining information on 110,000 and 12,000 individuals respectively (see ‘Ebb and Flow of the Campaign to Plug Offshore Tax Leakage’ Financial Times 6 May 2006; ‘Investigators Turn to Treasure Islands’, Sydney Morning Herald 9 September 2006). Although clearly successful in gaining access to substantial amounts of personal financial data, convictions for tax evasion stemming from this windfall have as yet been rare. The total sums of back taxes collected are also modest, so as an exercise in promoting tax compliance the effectiveness of this method is still unproven.
MONEY LAUNDERING

Money laundering is the process of obscuring the illicit origins of funds derived from crime. While the struggle between rulers and ruled over tax revenue is centuries old, money laundering has only been on the policy agenda for a little over 20 years (Gilmore 1995). No single policy priority has had a greater impact in eroding financial privacy. The current emphasis on countering money laundering first derived from the ‘War on Drugs’ in the 1980s (Naylor 2004). The international drug trade generates vast profits, and also requires substantial sums for working capital. To the extent that by criminalizing money laundering, authorities could ‘follow the money’ to attack the underlying crime, they could both attenuate the profit motive that drives drug crime, and disrupt the flow of working capital. In practice things have not proved so straightforward, with major uncertainties about the effectiveness of current anti-money laundering (AML) policy (Cueller 2003; Reuter and Truman 2004). Yet in terms of the extent of its diffusion, AML has been a runaway success story, with over 170 countries committed to meeting international standards in this area (FATF 2007a). The international standards in question have been designed predominantly by the FATF, a club of rich countries with a few strategically important developing nations, and by the FATF’s eight regional offshoots (one each in the Caribbean, Asia/Pacific, Europe, West Africa, Latin America, Eastern and Southern Africa, the Middle East, and Eurasia).

Just as financial privacy hinders governments’ efforts to collect taxes, it also complicates efforts to counter money laundering. Policies introduced to fight this type of crime have had a major impact on people’s everyday financial affairs. Even more so than the OECD in relation to tax policy, the FATF has dominated standard-setting in this area, with its 40 Recommendations on money laundering and 9 Special Recommendations on the financing of terrorism (FATF 2004; for details on how the Recommendations have been transposed into US legislation, see FATF 2006a; for the UK, see FATF 2007b). At the heart of AML regulation is the injunction for private financial institutions: ‘Know Your Customer’. These firms must also supply a steady stream of information to the authorities as part of the Suspicious Transactions Reporting regime. Relating to the former, opening a bank account now requires multiple sources of official identification: passport, national identity card where relevant, driver’s licence, utilities bills, and so on (Recommendations 4–10). Banks and other private institutions have a duty to report all suspicious transactions by their customers to the authorities, or be held civilly and criminally liable for failing to do so (Recommendation 2, 11, 13–16 and Special Recommendation 4). The criteria for what makes a transaction suspicious are hard to pin down, but seeking to bank a suitcase full of cash would certainly qualify (although there is no minimum threshold amount for reporting suspicious transactions). Other indicators might be moving money rapidly through a series of accounts, atypically large transactions, and transacting with individuals, firms or even countries that are themselves under suspicion of laundering money. Banks and other reporting institutions in the private sector are barred from telling customers that they have been the subject of a Suspicious Transaction Report (the prohibition against ‘tipping off’, Recommendation 14), and there is no involvement by the courts. Reporting firms are explicitly absolved from breaches of fiduciary responsibilities in fulfilling their reporting duties. Indeed, the duty to report suspicious transactions has superseded the lawyer-client confidentiality privilege in the UK, though attempts to do the same in Canada have been defeated in the courts as being contrary to the Charter of Rights and Freedoms.
As part of the more generalized requirement to Know Your Customer, the priority for those fighting money laundering is to make sure the parties to every transaction can be identified and traced (Recommendations 5 and 33). This requirement has meant reshaping laws that govern the simplest kinds of transaction, those involving cash, as well as the complex operations involving various kinds of corporate vehicles. Although new, anonymous electronic media of exchange have been developed, cash provides a perfectly anonymous means of transacting. In the name of fighting money laundering, countries have sought to penetrate this anonymity. The most direct response is to ban the use of cash in large transactions. Italy and France have forbidden cash transactions above €10,000, thereby forcing people and firms to use traceable electronic means of payment (UK Home Office 2003). Most countries, however, have rejected this approach as too drastic. Instead, they have imposed a duty on a widening circle of institutions (at first banks, then other financial firms, now casinos, real estate agents, jewellers, and so on) to report the identity of customers making large cash purchases (Recommendation 12). In most countries it is also now incumbent on travellers entering or exiting the jurisdiction to declare to the authorities if they are carrying more than a certain amount of cash, and provide a reason for travelling with such a sum (Special Recommendation 9).

Moving from the simple expedient of cash, those seeking financial anonymity for legitimate or illegitimate means have had a wealth of options in terms of different corporate vehicles (including companies, trusts, limited liability corporations, partnerships and foundations). To provide transparency in this area, there is now a general presumption (fostered in particular by the FATF and OECD) that the ‘beneficial ownership’ of any corporate vehicle must be established. This is a complicated area, and this article will only consider the basic issues at stake. Even in a world of perfect bank transparency, it is argued, criminals could still use the banking system by opening accounts in the names of companies whose ownership was untraceable. Thus, finding that account number 123456789 is held in the name of XYZ company provides little help in creating financial transparency if there is no information on who actually owns or controls XYZ company (UN 1998). Despite assumptions that companies must have employees, physical buildings and produce goods and services, companies and other corporate vehicles are in an important sense nothing more than a alternative legal identity for one person or a group of people. Companies can be set up online in a wide variety of OECD and non-OECD countries for as little as a few hundred dollars. Either deliberately or incidentally, companies can be used to provide a cover or screen for the identities of those persons enjoying ownership or exercising control (OECD 2001; FATF 2006b). One method is to issue company shares in bearer form, that is, where there is no central share registry and whoever physically holds the shares certificates owns them, just like cash. Thus if company XYZ has issued bearer shares, it is impossible for authorities to find out who owns the company short of physically finding the paper share certificates, which might be held in a bank safety deposit box in another jurisdiction. To defeat such obstacles, regulations to establish beneficial ownership require that, for example, authorities can find out not only that account number 123456789 is held in the name of company XYZ, but also that company XYZ is owned by Jane Smith, or (to give another example) Osama bin Smith.

The last issue in this section is the extent to which information gathered for the purposes of countering money laundering can be exchanged among different government agencies, at home or abroad. Summits of the G7 have urged countries to make AML information available for tax purposes (OECD 2002; Zagaris 2003). Once again in the position of
role model, in Australia, over 34 agencies can routinely access AML data, including
the Australian Tax Office, the bodies responsible for intelligence, unemployment, immigration, child support, customs, consumer protection and separate state bodies (Austrac 2007, p. 146). The flow of personal financial data between government agencies in most other countries is more constrained. Demonstrating the strong trust relations that bind together the transnational AML network, however, a variety of informal practices have been developed in response to these constraints. Agencies routinely coach their foreign counterparts on how to word information requests so as to work around local data protection laws. In some cases these bodies simply pass information illegally, particularly in response to requests from powerful outsiders. A counter to official prohibitions on sharing financial data domestically is for government agencies to come to an informal triangular exchange agreement: a trusted foreign counterpart agency is prompted to ask for certain information from domestic agency A, and then the foreign agency passes this same information to domestic agency B, circumventing the prohibition on A and B directly sharing data (Interviews, various Financial Intelligence Units). After the terrorist attacks of September 11, however, many governments have dropped earlier objections to sharing data between different bureaucracies, often rendering these informal work-arounds within the transnational AML community unnecessary.

THE FINANCING OF TERRORISM
At first sight, defeating al-Qaeda and other terrorist groups would seem to be far removed from the issue of financial privacy. But from almost immediately after the September 11 attacks, the Bush administration and the international community at large defined countering the finance of terrorism as an essential front in the fight against terrorism in general (Council on Foreign Relations 2002; Council on Foreign Relations 2004; Regan 2004; Bignami 2007). The United Nations Security Council passed Resolutions 1373 and 1390 to freeze and confiscate assets used to support terrorist activities. Despite the important differences between collecting taxes or countering money laundering on the one hand, and disrupting terrorist finance on the other, in practice the policy implications for financial privacy are very similar. The nuts and bolts of countering the finance of terrorism have tended to follow very closely the procedures instituted for countering money laundering (Know Your Customer, suspicious transaction reporting, lists of suspicious individuals, and so on) summarized earlier. The overlap is so pronounced that the two have become fused under a single acronym: AML/CFT. Working from its anti-money laundering remit, the FATF has also become the standard-setter in countering terrorist financing (but see also IMF/World Bank 2005). Once again, privacy is seen as an obstacle to achieving state goals, in that to the extent governments cannot freely access financial information, they cannot identify, block and seize terrorists’ funds. Once again, new policy measures in this area have generally allowed governments to access and collect more private financial data, and share these data more freely between different government agencies.

The moral resonance of rhetoric about fighting terrorism has been a powerful tool for rebutting or silencing those who would restrict governments’ access to personal financial data. Banks and other financial institutions are generally reluctant to complain about the costs of the AML/CFT regulations for fear of being portrayed as ‘soft on terrorism’ (Naylor 2004). Reflecting a commonly held attitude, a senior PricewaterhouseCoopers executive noted: ‘Post-September 11, I don’t think it’s acceptable for any finance centre to
say that they value banking secrecy more than human life’ (International Tax Review May 2002).

Immediately after September 2001, the US executive established the Terrorist Finance Tracking Program (Privacy International 2006). The program centred on secretly obtaining data from the SWIFT (Society for Worldwide Interbank Financial Telecommunications) network, by which international bank-to-bank transfers are processed. SWIFT, a Belgian-based co-operative, passes an average of 10 million messages transferring $6 trillion each day (see http://www.swift.com/). Working in co-operation with the CIA, the US Treasury Department’s Office of Foreign Asset Control approached SWIFT in October 2001 with special administrative subpoenas issued under the US International Emergency Economic Power Act. Paralleling the modus operandi of the OECD on tax and FATF on money laundering, the US government had a clear preference for administrative procedures rather than taking the conventional route of going to court to obtain a warrant or normal subpoena. Once the program became public after media leaks in 2006, US government officials maintained it was narrowly targeted. But the New York Times piece which broke the story spoke of 64 subpoenas issued between 2001 and 2006 relating to ‘tens of thousands’ of banking transfers relating to ‘thousands’ of individuals (including names and account numbers).

The Under-Secretary of the Treasury responsible for the monitoring program said unequivocally: ‘People do not have a privacy interest in their international wire transactions’ (‘Bank Data Sifted by US in Secret to Block Terror’, New York Times 23 June 2006). When initially approached by the US Treasury, SWIFT asked for guidance from its supervisory board of the Belgian, British and European Central Banks, who were thus aware of the program well before it became public knowledge in mid-2006. The transnational central bank community was unwilling to provide any advice, but was also apparently unwilling to reveal the existence of the program to governments or the European Commission. The European Central Bank later explained that data protection was not its responsibility (ECB Press Release 1 February 2007), a point explicitly rejected by European data protection commissioners. US access to SWIFT data continues, but European banks are now obliged to alert their customers to this fact (‘Europe’s Banks Must Inform Customers of US Snooping’, Register 27 June 2007).

CONCLUSION

This article has argued that there is a right to financial privacy, but that in practice this right has become significantly eroded. New measures to counter tax evasion, money laundering and the financing of terrorism have relied on the same kinds of instruments. They have all been animated by the same underlying premise that financial transparency is essential in responding to these interlinked problems. The dominance of the principle of transparency, justified on the grounds of a ‘nothing to hide, nothing to fear’ logic, and the equation of privacy with roguery, mean that the decline of financial privacy looks set to continue. The key actors driving change have been transnational regulatory networks responsible for drawing up international standards in this area and socializing those in national governments responsible for translating these non-binding guidelines into binding policies. Too often it is assumed that these networks and international organizations are merely faithful extensions of their component national governments, undertaking technical tasks of little political import. In fact, they may enjoy considerable autonomy and substantial indirect influence over national policy. They do so through the
exercise of classic bureaucratic prerogatives: rational-legal authority and the privileging of functional efficiency.

What might be lost if the diminution of financial privacy continues? Westin notes that privacy underpins democracy; once individuals lose the ability to control their personal information ‘we have, in very concrete terms, lost our rights to decide when and with whom we choose to speak, publish, worship and associate’ (Westin 2003, p. 249). Decisions about when and with whom to exchange ideas and associate can often leave financial traces: Internet subscriptions, books bought, membership in or donations to political parties and non-governmental organizations. Thanks to the increasing tendency to buy goods and services that would previously have been produced at home, and even more so the rise of electronic transactions, more and more of our decisions and behaviour become recordable, searchable data. Recent writings on the significance of state surveillance, the ability of the state to make society transparent and ‘legible’, or the ubiquity of power as self-discipline in a ‘panoptic’ social structure, all argue for the fundamental importance of the politics of privacy (Foucault 1975; Gandhi 1993; Scott 1998). In these accounts, the struggle for control of individuals’ personal information is central to the development of modern states and societies, through tools such as the census, property register and tax roll. The technological and policy changes that for the first time have made the majority of personal consumption and financial transactions able to be accessed, collected and archived by the authorities extend this dynamic to important new terrain. Past contests over the state’s attempts to know those under its authority and their dealings have had implications far beyond narrow technical concerns, as society was re-shaped along new lines. With this history in mind, the future ramifications of current policies relating to financial privacy may extend far beyond the relatively narrow goals that have justified their introduction.

ACKNOWLEDGEMENT

This article draws upon interviews conducted by the author with members of the OECD Committee on Fiscal Affairs and the FATF. The author would like to thank the participants in the European Consortium on Political Research Joint Session ‘Privacy and Information: Modes of Regulation’ organized by Andreas Busch and Charles Raab, held in Helsinki, May 2007. The author also gratefully acknowledges the support of the Australian Research Council Discover Grant (DP0771521).

REFERENCES


FATF. 2007a. President’s Address, Strasbourg Plenary, 19–23 February.


*Date received 6 July 2007. Date accepted 17 March 2008.*
USING E-ANNOTATION TOOLS FOR ELECTRONIC PROOF CORRECTION

Required Software
Adobe Acrobat Professional or Acrobat Reader (version 7.0 or above) is required to e-annotate PDFs. Acrobat 8 Reader is a free download: http://www.adobe.com/products/acrobat/readstep2.html
Once you have Acrobat Reader 8 on your PC and open the proof, you will see the Commenting Toolbar (if it does not appear automatically go to Tools>Commenting<Commenting Toolbar). The Commenting Toolbar looks like this:

![Commenting Toolbar](image)

If you experience problems annotating files in Adobe Acrobat Reader 9 then you may need to change a preference setting in order to edit.
In the “Documents” category under “Edit – Preferences”, please select the category 'Documents' and change the setting “PDF/A mode” to “Never”.

PDF/A View Mode

View documents in PDF/A mode: Never

Note Tool — For making notes at specific points in the text
Marks a point on the paper where a note or question needs to be addressed.

![Note Tool](image)

How to use it:
1. Right click into area of either inserted text or relevance to note
2. Select Add Note and a yellow speech bubble symbol and text box will appear
3. Type comment into the text box
4. Click the X in the top right hand corner of the note box to close.

Replacement text tool — For deleting one word/section of text and replacing it
Strikes red line through text and opens up a replacement text box.

![Replacement Text Tool](image)

How to use it:
1. Select cursor from toolbar
2. Highlight word or sentence
3. Right click
4. Select Replace Text (Comment) option
5. Type replacement text in blue box
6. Click outside of the blue box to close

Cross out text tool — For deleting text when there is nothing to replace selection
Strikes through text in a red line.

![Cross out Text Tool](image)

How to use it:
1. Select cursor from toolbar
2. Highlight word or sentence
Approved tool — For approving a proof and that no corrections at all are required.

How to use it:
1. Click on the Stamp Tool in the toolbar
2. Select the Approved rubber stamp from the 'standard business' selection
3. Click on the text where you want to rubber stamp to appear (usually first page)

Highlight tool — For highlighting selection that should be changed to bold or italic.

How to use it:
1. Select Highlighter Tool from the commenting toolbar
2. Highlight the desired text
3. Add a note detailing the required change

Attach File Tool — For inserting large amounts of text or replacement figures as a file.

How to use it:
1. Click on paperclip icon in the commenting toolbar
2. Click where you want to insert the attachment
3. Select the saved file from your PC/network
4. Select appearance of icon (paperclip, graph, attachment or tag) and close

Pencil tool — For circling parts of figures or making freeform marks

How to use it:
1. Select Tools > Drawing Markups > Pencil Tool
2. Draw with the cursor
3. Multiple pieces of pencil annotation can be grouped together
4. Once finished, move the cursor over the shape until an arrowhead appears and right click
Help
For further information on how to annotate proofs click on the Help button to activate a list of instructions: