Appendix 2

LL.M. in International and European Law
RESEARCH PROJECT

Jean Moulin University Lyon 3

The ever-increasing cross-border exchange of tax information between governments: Does this result in breaches of privacy rights? What are the implications of such breaches and what protective mechanisms should be put in place?

Student: William Ahern

Director: Professor Lukasz Stankiewicz

Date of Submission: 8 March 2012

1. INTRODUCTION

It is necessary for personal information to be transferred to governments for tax collection purposes in exchange for an individual's participation in democratic society and the benefits gained from such participation. To this extent, certain informational privacy is voluntarily forfeited. This voluntary forfeiture however is predicated on the basis that that information will be protected from misuse by the State and its various legal regimes and mechanisms. Can one be sure in that belief with regards to information that is then passed by national governments to other foreign governments pursuant to cross-border tax information exchange agreements?

Recent times have seen a proliferation of Tax Information Exchange Agreements (TIEAs) signed between countries and by "enhanced" exchange of information provisions in existing and new comprehensive double tax agreements ("CDTA's") collectively hereafter referred to as TIEA's. In general, tax information exchange between countries should be a sensible and powerful deterrent against tax evasion by those seeking to avoid paying taxes by hiding their money in other countries. However, it is essential that TIEAs do not lead to the breach of taxpayer's right to informational privacy and abuses resulting from such breaches. TIEAs contain varying provisions aimed at safeguarding against such breaches and abuses. Are the protective provisions adequate? Can all parties to such agreements, some of which are countries with poor governance records, be entrusted to abide by them?

This paper concludes that whilst certain protections exist in the TIEA's themselves, in other bilateral agreements on the protection of personal information and data transfers and in the domestic laws of various countries, there is significant room for improvement in those protections.

It then sets out a number of detailed recommendations for improvement.

2. THE CONCEPT OF INFORMATIONAL PRIVACY

It is useful to examine the nature and basis of rights to informational privacy at law, including the different types of private information. It is well known that attempts to define or articulate the concept of privacy have been met with

considerable difficulty.[1] Richard Posner, one of the most well known American legal writers on privacy, describes the concept of privacy as "illusive and ill defined". It has been argued that one reason for this difficulty is that privacy is not purely a legal term, it is impacted by political, economic and technological influences and as a legal right is intertwined with many other legal areas.[2]

The first publication, in America at least, arguing for a privacy right was that of Warren and Brandeis in 1890[3] who described that right as "the right to be let alone" a right which they argued was based in natural law. Their paper was focused on the right to keep one's private information secure and was a reaction to changing trends brought about in part by developing technologies. The changing trend was an increase in the circulation of newspaper articles and photographs revealing information of a personal nature about individuals, due to developments in printing technologies. This paper focuses on an increase in cross-border exchange of private information by governments; particularly tax information, which has been brought about in part by developing internet and database technologies. This paper will argue that now, as in the time of Warren and Brandies, sudden changes in circumstances, which include new technologies, globalization more generally and an increased desire by governments to share tax information[4], have brought about the need for a legal response.

The different conceptions of privacy were examined by Lawrence Lessig[5]. The first conception Lessig refers to is the utility conception that relates to the burden of intrusion. An example is a police search of one's property that creates a burden or inconvenience. The second conception is one of dignity. While an intrusion into a person's home by a journalist of which the victim is unaware may not create a burden, it will intrude upon their dignity. The third conception identified by Lessig and perhaps the most relevant to the subject of this paper is what he calls the substantive conception of privacy. This considers privacy concerns as a way of constraining the

---

[1] Posner R. A, "The Right of Privacy", *Georgia Law Review*, Vol. 12, No.3 (1978).
[2] Elkin Koren, N & Birnhark, M, "Privacy in the digital Environment", *The Haifa Centre of Law and Technology Publication Series*, Publication No. 7 (2005).
[3] Warren & Brandeis, "The Right to Privacy" *Harvard Law Review*, Vol. 5, No. 5, (1890).
[4] Cockfield, J A. "Protecting Taxpayer Privacy Rights under Enhanced Cross-border Tax Information Exchange: Toward a Multilateral Taxpayer Bill of Rights" *University of British Columbia Law Review*, Vol. 42, pp. 420-471 (2010)
[5] Lessig, L. "The Architecture of Privacy", *Van. J. Ent. L. & Prac*. 56 (1999).

power of the state to regulate and to restrict the scope of regulation that is possible. The question at hand, one relating to informational privacy, is initially one that concerns the power of the state to regulate more so than questions of burdens, intrusion or dignity, however when this information is passed on to those with an intention to abuse such information, questions relating to burden and intrusion come into play.

Informational privacy can be distinguished from other forms of privacy protected at law that will not be examined in detail in this paper, but which include physical privacy, organizational privacy and emotional and intellectual privacy. A crucial element of informational privacy is the element of control over the collection and dissemination of information. Information privacy was described by Westin as the "*claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others*[6]*."* This definition is helpful in its articulation of the element of determination by holders of information of how and to whom information is shared. It does not however address, as others have,[7] the ability to control the entire information flow process, including its collection. Miller states that:

> *"[T]he basic attribute of an effective right to privacy is the individual's ability to control the flow of information concerning or describing him -- a capability that often is essential to the establishment of social relationships and the maintenance of personal freedom."*

It is relevant then to examine the different types of private information that may be subject to protection under the law and how this information is obtained, i.e. voluntarily or otherwise, and how this may impact upon one's right to privacy. The different types of digital personal information that can be collected by government include tax information, customs, criminal or immigration data. Information that is collected by the private sector but which also may become available to governments includes information such as records of purchases[8]. These various sources of information are available to governments today as a result of rapid technological developments and when pieced together can provide a detailed profile of an individual

---

[6] Westin, A, F. "Privacy and Freedom", 25 *Wash. & Lee L. Rev.* 166 (1967).
[7] Miller, R, A. "The Assault on Privacy: Computers, Databanks, and Dossiers" *U. ILL. L.F*, 154, 168 (1971).
[8] Cockfield *supra* note 4 at 8.

that provides governments with the tools to use such information beyond the original tax collecting purpose, such as for a criminal investigations, political purposes or when in the hand of criminals, kidnapping or identity theft[9].

Financial Privacy in Particular

Financial privacy has been defined as the "ability, and what many consider the right, to keep confidential the facts concerning one's income, expenditures, investments and wealth[10]". Financial details and information can reveal a lot about a person, including their social status, activities, preferences and personality[11]. There are many different reasons why people may wish to avoid others having access to facts that reveal their financial status. These may include a desire to avoid being compared to others due to their financial status[12] or to avoid interference with their creativity and autonomy[13]. A fear that has particular relevance to the issues at hand in this paper is one that political enemies, or enemies in general, will use their financial information to their detriment, by way of embarrassment, discreditation, or worse. Motivations for keeping financial information private may also include a desire to be free from solicitation, either by persons one knows, such as friends or family, or commercial solicitation[14]from the sellers of goods and services. People may also wish to keep financial information private from creditors and such information may assist in the enforcement of, for example, debts, liabilities and fines[15].

Another important concern for the purposes of this paper, along with that of political persecution, is a fear that information about a person's wealth may lead to them becoming targets of criminals including thieves and kidnappers[16]. Blum addresses how these fears may be justified by detailing how information relating to a

---

[9] *Id* at 9.
[10] Richard W, R. "The Future of Money and Financial Privacy, in The Future of Financial Privacy-private choices versus political rules", *The Competitive Enterprise Institute,* ed. 126, 132 (2000).
[11] Blum, C. "Sharing Bank Deposit Information With Other Countries: Should Tax Compliance or Privacy Claims Prevail?" *Florida Law Review,* Vol. 6:6(2004)
[12] Linder, M." Tax Glasnost for Millionaires: Peeking Behind the Veil of Ignorance Along the Publicity-Privacy Continuum," *N.Y.U. Rev. L. & Soc. Change* 951, 971 (1990/1991).
[13] Blum *supra* note 10 at 604
[14] *Id* at 605
[15] *Id*
[16] Posner, R. "The Economics of Justice", *Harvard University Press,* 234-35 (1983)

person's finances can reveal considerable additional information about that person's activities. She states that an individual's receipts or expenditure can reveal information about a person's "material possessions, spending or saving habits, obligations, occupation, abilities, associations, beliefs, interests, and personality". She highlights as examples records that might indicate such information including payments to political parties or charities, purchases of particular brands, payments of child support and records of purchases that will indicate one's locations such as flights or hotel reservations. Cockfield[17] states that taxpayer information "is a particularly sensitive form of personal information, and can be used to build a detailed profile of individual identity, including religious and political beliefs" while a US Judge stated that "the banking transactions of an individual give a fairly accurate account of his religion, ideology, opinions and interests[18]".

3. IN WHAT WAYS ARE INFORMATIONAL PRIVACY PROTECTED AT LAW?

A. USA

A useful starting point in examining the legal developments in informational privacy is the US, which is one of the major contributors to the recent proliferation in cross-border tax information exchange due to its influential position within the OECD. In the US there exists a tort right to information privacy that protects the unauthorized acquisition of personal or intimate information that is known as the Privacy Intrusion tort[19]. This is in addition to the earlier Public Disclosure tort that deals with losses of privacy by dissemination of information by the media[20]. Both of these torts are viewed as having their origins in the Warren and Brandies article referred to earlier in this paper[21].

More important to the issues at hand in this paper are federal constitutional rights that individuals have against government. The most traditional sources of constitutional rights protecting informational privacy are those found in the fourth

[17] Cockfield *supra* note 7.
[18] California Bankers Ass'n v. Schultz 416 U.S. 21 (1974),
[19] Turkington, R. C, "Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy" 10 *N. Ill. U. L. Rev*. 489 (1989-1990).
[20] *Id* at 490
[21] *Id* at 493

amendment with respect to search and seizures[22]. This right to privacy under the fourth amendment is of course irrelevant for the purposes of arguments to be made in this article as it can only be invoked in situations where the information in question is acquired by a government search.

Relevant to arguments to be made in this paper is what is referred to by Turkington[23]as an "emerging unencumbered constitutional right to informational privacy" after US Courts found that there may be a right to informational privacy under the due process clause of the Fourteenth Amendment. A number of cases in various US Courts have examined whether there is a constitutional right to informational privacy under the Fourteenth Amendment and whether such a right is breached by publication or dissemination by government. The first such case was that of *York v Story*[24] heard by the Ninth Circuit which was the first Court to hold that governmental encroachment on informational privacy other than via a search violated the constitutional right to informational privacy.

The Supreme Court famously considered the question in *Whalen v Roe*[25] in a case brought by doctors and patients challenging a New York statute requiring copies of certain prescriptions to be recorded in a government computer. The claim was that this violated their constitutional right to privacy. While the Court rejected the claim it theorized that in certain circumstances the collection and disclosure of such information might violate the constitutional privacy rights of patients. In that case informational privacy, that being avoiding disclosure of personal matters, was identified for the first time as one of two branches of constitutional rights to privacy.

Importantly for some of the questions to be raised in this article, Justice Stevens at paragraph 605 of that decision stated:

> *"We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files .... The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing*

[22] *Id*
[23] *Id* at 495
[24] 324 F.2d 450 (9th Cir. 1963).
[25] 429 U.S. 589 (1977).

that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme ... evidence[s] a proper concern with, and protection of, individuals ...."

The issue was revisited more recently by the Supreme Court in the case of *NASA v Nelson*[26]where NASA employees challenged regulations that required background checks for employees of federal government contractors, including questions about drug use, mental health, and financial status. Their arguments included that the regulations breached their constitutional right to privacy under the due process clause. Whilst the Court found that the information gathering in this instance did not breach such a right, if it existed, a clear majority of the Court reached its decision on an assumption that it may, clearly leaving the question open for future exploration.

In reaching its decision the Court balanced the importance of the right against the importance of the information gathering to the government and the presence of measures in place that secure, or keep private, the information following its collection. In this case the measures examined where contained within the US Federal Privacy Act[27].

Turkington[28] sets out the central features of the balancing test that the Court has developed in cases such as the two described above. He rightly points out that as a condition for receiving benefits and services from the government people must provide it with information. For a government to be able to perform its duties a large amount of information must be collected and disseminated and as such Courts have been hesitant when hearing claims of breaches of informational privacy by government.

The first element of the test is an evaluation of the extent of the invasion of privacy as weighed against an evaluation of the need for the collection and/or dissemination of the information by government. He identifies a threshold question that asks "Is the information acquired intimate or of a personal nature". The right to constitutional informational privacy can only be invoked if the information acquired, or relevantly to the question at hand in this paper, disseminated, is of a kind legally

[26] 530 F.3d 865
[27] *1974*
[28] Turkington *supra* note 20 at 505

and socially recognized as "significantly implicating privacy". He identifies two important factors when considering if information is of such a character, those being 'intrinsic' and 'consequential' features of the information. Intrinsic features refer to the level of intimacy of the information whilst consequential refers to the potential for harm upon disclosure. It is identified that information of a personal nature may not be intimate but may be subject to protection as harmful consequences may result from dissemination. The article states:

> *"disclosure of information about assets or liabilities could result in unwanted solicitation from various sources and encourage lawsuits or other harassing activities, including the possibility of being subject to extortion or kidnapping".*

Under this definition it could be said that tax information disclosed to foreign governments under TIEAs reaches the threshold of information 'significantly implicating privacy'.

The next question raised is whether the intrusion is justified. When examining the question of justification due to the public or government interest it can be useful to draw comparisons between possible breaches of informational privacy under TIEAs with countries that fail to provide adequate privacy protection and challenges brought in American courts against financial disclosure laws by government employees. There have been limited occasions where US Courts have found that financial disclosure legislation relating to public officials have breached a federal constitutional right to informational privacy[29]. In most of these cases courts have found that compelled disclosure of this information invokes the right to informational privacy but usually that such laws were justified due to the public interest[30]of deterring corruption and maintaining confidence in government. The courts have found that government employees have less constitutional protection than private sector employees[31].

Perhaps with some difficulty an argument can be made that public interest factors in cases of financial disclosure are greater than those with respect to tax information exchange or conducting tax information exchange with countries that cannot provide for privacy of transferred information. Less difficult to make is an argument that the government's ability to keep information safe from misuse under

[29]*See City of Carmel-by-the-Sea v. Young,* 2 Cal. 3d 259, 466
[30] *See* for example *Belle Bonfils,* 763 (Colo. 1988)
[31] Turkington *supra* note 20 at 515.

TIEAs is less than that under financial disclosure laws. With respect to financial disclosure laws, that information is made available within the US. Any misusers of that information are then subject to US law and the persons required to disclose the information are subject to protection under US law.

This article argues that TIEAs with countries that are unable to provide adequate protection to the privacy of taxpayer information endanger privacy rights. It is not argued that this is this case for all tax information exchange provided that adequate protection can be guaranteed. Hence a balancing exercise of the public interest against the constitutional right to privacy for the purposes of this article is one that balances the public interest gains of pursuing TIEAs with countries potentially unable to provide adequate protection against the individuals constitutional right to informational privacy.

It is apparent that the push for and recent proliferation of TIEAs was brought about by the concern of OECD nations that tax revenue was being lost due to undeclared or hidden earnings and activities in International Financial Centers (IFCs), and tax havens. An argument could be made, and has made by many recent scholars[32], that tax havens in fact play a positive role in the world economy and in the efficiency of national tax systems. These positive influences, it is argued[33], include increased foreign direct investment in high-income countries. There is of course a countervailing view that tax havens are 'parasitic' on the tax revenues of non tax haven countries that in turn reduce the welfare of their residents[34]. However the arguments of this paper are restricted to those which favor a revised approach to the structure of TIEAs in their current form and the safeguards in place that govern privacy protection under them, rather than an end to tax information exchange in general. In fact due to reasons discussed in the following paragraph a discussion of whether or not tax havens are beneficial or harmful to other countries is irrelevant for the purposes of this article.

---

[32] See Desai, Mihir A., C. Fritz Foley, and James R. Hines Jr., Do tax havens divert economic activity?" *Economics Letters*, (2006), 90 (2), 219-224; Desai, Mihir A., C. Fritz Foley, and James R. Hines Jr., The demand for tax haven operations, *Journal of Public Economics*, 513-531 (2006), 90 (3) pages.

[33] Hines R J, "International Financial Centers and The World Economy", *STEP Report,* 11 (2009) page 11

[34] Slemrod J, "Why Is Elvis on Burkina Faso Postage Stamps? Cross-Country Evidence on the Commercialization of State Sovereignty", *Journal of Empirical Legal Studies, Volume 5,* Issue 4, 683–712 (2008)

One feature that may balance the public interest argument in favor of the right to informational privacy against pursuing TIEAs with countries that cannot provide adequate safeguards is that in the vast majority of cases tax havens are not among those countries that are categorized as having poor governance[35]. Evidence in fact suggests that US firms are attracted to and in turn invest additionally in countries with both good governance and low taxes but that levels of investment do not increase significantly in countries with both low taxes and poor governance[36]. If this is indeed the case then the public interest in pursuing TIEAs with such countries is diminished due to the relatively low level of tax revenue lost. The fact that countries that would be precluded from participating in TIEAs that contained greater safeguards and standards relating to privacy do not include the majority of IFCs and tax havens diminishes any public interest argument against imposing greater safeguards and standards.

If a case were brought by a party claiming a breach of its constitutional right to privacy due to the dissemination by the government of private information pursuant to a TIEA, what would be examined under such a balancing exercise? It is not disputed that there is considerable importance in a government's desire to receive financial information about its citizens in other jurisdictions in order to identify and deter tax avoidance. The importance of such activities are however different than the need for domestic collection of tax information of each citizen for the purposes of national tax administration. The statutory and regulatory regimes in place regulating the dissemination of tax data from the IRS to other government agencies is greater than those in place under TIEAs. In fact tax data is subject to significant protection in the US and there are significant restrictions upon when and how tax return information can be shared with other governmental agencies by the IRS[37].

US Courts have identified, when considering challenges against financial disclosure laws, that privacy rights are effected more adversely in the dissemination of that information to the public than in its initial collection[38]. The possible invasion

---

[35] Hines *supra* note 33 at 11
[36] Dhammika D & Hinse R J, "Why Do Countries Become Tax Havens?" NBER Working Paper No. 12802, (2009)
[37] Slemrod J, 'Taxation and Big Brother: Information, Personalisation and Privacy in 21st Century Tax Policy', *Fiscal Studies*, vol. 27, no. 1 (2006).
[38] Barry v. City of New York, 712 F.2d 1554 (2d Cir. 1983)

of privacy in a case relating to tax information exchange would not be in the collection of the data but the dissemination of it offshore. When we are speaking about tax information exchange can we be confident that there are measures in place in the destination country to avoid unwarranted disclosures? If the Court is saying that government is able to forgo its constitutional, or at least statutory, duty not to disseminate the information it collects from citizens when the *"right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures"* then the question must be asked whether the protection provided by the government to its taxpayers when disclosing information to foreign governments meets the standards that allows it to forgo its duty not to disseminate.

It could be argued that once that information has been sent offshore there is no way that the government could guarantee such protections as the information is not then subject to internal statutory or regulatory duties to avoid unwarranted disclosure. Instead it must rely on the authorities in the country of destination of the information. This is of particular concern when considering that in certain countries in which the US and other countries have entered into TIEAs such statutory or regulatory protections may be weak. It is true that the TIEAs themselves address mechanisms aimed at addressing such concerns. Whether these are sufficient will be addressed later in the paper when TIEAs will be addressed in detail. Whether they provide for protection of taxpayers informational privacy that is equivalent to that which is statutorily guaranteed in the US is doubtful.

The Internal Revenue Code[39] (IRC), particularly Section 6103 of that Code provides that the US Internal Revenue Service (IRS) can have access to personal financial information required to enforce the national income tax. The secrecy of this information is protected by the Statute but may be disclosed in certain situations that are also set out in the Statute. Blum sets out[40] certain situations in which a taxpayer's private information may be misused within the US. These include public disclosure or use by IRS employees, the loss of political or financial advantage and the suffering of oppression at the hands of the government. Furthermore, there are concerns about the effect upon liberty in general that comes from the large volume of financial data

[39] 26 U.S.C
[40] Blum *supra* note 10 at 616

available to the IRS[41]. Blum points out that these concerns have not been generally heeded by the US Congress, which has in fact allowed for, through Section 6103 of the IRC, for the IRS to disclose personal tax information to other agencies for purposes other than tax administration, albeit with a system of safeguards[42] in place surrounding such disclosures. Examples of such disclosures from the IRS to other government agencies include to the US Customs Service, agencies administering welfare programs and to child support agencies.

It is within this context that Blum explores the question of why it is then controversial that US Government would routinely transfer information with other countries[43]. Blum addresses the issue[44] not only from the perspective of a breach of privacy rights of US citizens who have had their information sent-offshore, as this paper has so far been limited to, but also the privacy claims of "nonresident aliens with US bank accounts". It is noted that it is fairly unlikely that the IRS will abuse or disclose information held by it without being permitted to do so by statute and that the stability or quality of governance in the US may be one of the reasons the nonresident has chosen to open a US bank account in the first place. The greater concern quite obviously is the transfer of information from the US tax authorities to those in the nonresident aliens country of residence, pursuant to IRC Section 6103(k)(4) which allows for disclosure under information exchange agreements.

It is stated that consequences of such disclosure could be severe if the recipient country's government was "oppressive, corrupt, unstable, or otherwise irresponsible". A list of possible consequences, some already listed in this paper, are then set out and include expropriation of funds and the leaking of information to criminals. Blum, in noting that such consequences would result in a breach to ones human rights suggests that an amendment to "IRC section 6103(k)(4) is needed so that IRS transmittal of tax information is restricted to countries that can provide assurance that the information will be safeguarded and will be used only for the purposes intended." This suggestion is one that is that is compatible with others to be made throughout this paper, which relate to not only the US and its IRC but to other

---

[41] Swire, P, P. "Financial Privacy and The Theory of High-Tech Government Surveillance", 77 *Wash. U. L. Q.* 461, 470 (1999)
[42] IRC 6103(p)(4),(5),(6)
[43] Blum's paper examines an at the time proposed IRS regulation that sought to allow automatic and spontaneous tax information exchange with certain governments.
[44] Blum *supra* note 10 at 624

jurisdictions and the regulation of tax information exchange in general. It must be noted however that Blum's suggestion is qualified with a statement that is sensible in setting out a balanced consideration of the issues at hand:

> *"On the other hand, a foreign government that demonstrates its actual adherence to appropriate standards for handling and using tax information should not be denied such information merely because it does not meet Western standards for political democracy; in some cases, securing a table revenue source may be a necessary step in progress toward greater political rights and rule of law"*

B. Privacy Law in Europe

Europe in particular has been a world leader in passing legislation aimed at protecting informational privacy. Such legislation is often referred to as dealing with data protection or fair information practices. The German state of Hesse passed the first legislation dealing with data protection in 1970, which was followed by the passing of the first of such national legislation in 1973 by Sweden[45]. Similar legislation followed nationally in Germany (1977), in France (1978) and then spread to many countries in Europe[46].

The beginnings of a framework for Europe wide protection against unfair collection and processing of data was seen in the adoption of Council of Europe Resolutions (73) 22 on the protection of the privacy of individuals vis-à-vis electronic databank in the private sector (1973) and (74) 29 on the protection of the privacy of individuals vis-à-vis electronic databank in the public sector.

In 1981 at around the same time that other international institutions such as the OECD were addressing privacy regulation (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) with a focus on international implications, the Council of Europe adopted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*[47] (Convention 108). That Convention was the first internationally binding instrument dealing with data protection. It draws on the *European Convention on Human Rights and*

---

[45] Cate, F. "The EU Data Protection Directive, Information Privacy and the Public Interest", *Iowa Law Review,* 80 (1995)
[46] *Id*
[47] Convention ETS No 108 of the Council of Europe (of 1981)

Fundamental Freedoms 1950 (ECHR), in particular Article 8 of the ECHR that states, "Everyone has the right to respect for his private and family life, his home and his correspondence". The ECHR further states that this right can only be restricted by a public authority in accordance with national laws as far as necessary in a democratic society for certain legitimate aims.

Contracting states to Convention 108 are obliged to implement national legislation that complies with the principles set out it in the Convention. The main principles set out in the Convention include fair and lawful collection and automatic processing of data, storage for specified legitimate purposes, and duration of storage of information. They concern also the quality, relevance and proportionality of the data, data accuracy, confidentiality of sensitive data, information of the data subject; and the right of access and rectification of data[48].

The Convention provides for free flow of personal data between contracting states to the Convention. This free flow can only be obstructed if parties derogate from the provision. The two cases in which parties can derogate are when protection of personal data in the other party is not equivalent, or the data is transferred to a third state that is not party to the Convention.

C. Data Protection Directive

The European legislative instrument most widely applied in the area of data protection is *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (Directive 95). The objectives of Directive 95 build upon Convention 108. The Directive was brought about by a need, identified by the European Commission, for data protection legislation within all EU member states to be uniform, in order to prevent the impediment of the free flow of data within the EU. The first objective of the European Data Directive is to ensure that member states protect the fundamental right of natural persons to privacy with respect to processing of personal data. The second is related to the prevention of the impediment, by member states, of the free flow described above[49].

[48]Council of Europe Website http://www.coe.int/t/dghl/standardsetting/DataProtection/History_more_en.asp

[49] Article 1 (1) & (2) of the Directive

While the Directive 95 may not be directly applicable to the issue of tax information exchange, it is the primary European mechanism for protecting data privacy. If TIEAs are inconsistent with the core principles of the Directive, questions must be asked as to why European countries are entering into TIEAs in their current form and with countries unable to provide adequate protection. An analysis of the relevance of Directive 95 to TIEAs and TIEAs compliance with Directive 95 is therefore necessary.

For the purposes of the directive 'personal data' is defined as "…any information relating to an identifiable person who can be identified in particular with reference to…one or more factors such as his physical, physiological, mental, economic, cultural or social identity". The information that is regularly exchanged under tax information exchange quite obviously falls within this definition. The OECD Model Agreement on Exchange of Information on Tax Matters (the Model Agreement) for example at Article 1 "Scope and Scope of the Agreement" states that:

> *"Contracting Parties shall provide assistance through exchange of information that is foreseeably relevant to the administration and enforcement of the domestic laws of the Contracting Parties concerning taxes covered by this Agreement. Such information shall include information that is foreseeably relevant to the determination, assessment and collection of such taxes, the recovery and enforcement of tax claims, or the investigation or prosecution of tax matters."*

Information is then defined at Article 4 (1)(m) of the Model Agreement as "any fact, statement or record in any form whatsoever." This is expanded on in the commentary of the Model Agreement which states that the definition of information under the Model Agreement is 'very broad' and that a "*Record includes (but is not limited to): an account, an agreement, a book, a chart, a table, a diagram, a form, an image, an invoice, a letter, a map, a memorandum, a plan, a return, a telegram and a voucher."*

The definitions set out in Directive 95 for "Processing of Personal Data' and 'Personal Data Filing Systems'[50] could clearly encompass the processing and filing systems used by tax authorities leading to tax information exchange. Additionally the definitions of 'Controller', 'processor', 'third party' and 'recipient' all contain the words 'public authority', which could clearly encompasses tax authorities.

[50] Article 2 (b) & (c) of the Directive

Article 3 of Directive 95, which sets out the scope of the Directive, contains at Article 3(2) a list of personal data that shall not apply. One of these is the activity of states in the area of criminal law. International tax information exchange is not caught by this exception as its scope goes well beyond that of the investigation of criminal tax matters. Article 1 of the Model Agreement states the information to be exchanged includes information "that is foreseeably relevant to the determination, assessment and collection of such taxes, the recovery and enforcement of tax claims, or the investigation or prosecution of tax matters." Section IV of Directive 95 sets out the various exemptions and restrictions. Article 13 (1) (e) of Directive 95 states that member states may adopt legislative measures to restrict the scope of obligations and rights relating to certain principles relating to data quality[51], the need for information to be given to the data subject[52], the data subjects right of access to data[53] and the publicizing of data processing operations[54] when "such a restriction constitutes necessary measures to safeguard" amongst other areas, "an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters." These Articles do not however provide a blanket exemption from the directive for tax authorities due to the nature of the information and the purposes that it serves. Importantly Article 13 (1) does not provide an exemption from compliance with the Directive's provisions relating to the transfer of data to a third country. These Articles are discussed in the proceeding paragraph.

Perhaps the most important provisions of Directive 95 with respect to the issues at hand in this paper are those under Chapter IV relating to the transfer of data to third countries. Article 25 (1) states that the transfer of personal data to a third country may take place only when the third country in questions provides an adequate level of protection. Article 25 (2) goes on to say that the adequacy of the level of protection afforded by a third party is to be assessed in the light of all circumstance surrounding the data transfer. Circumstances to be considered include the nature of the data, the purpose and nature of the processing, the country of origin and the final destination. Importantly, with respect to the destination country, Article 25 (2) states that consideration must be taken of the "…rules of law, both general and sectoral, in

[51] Specifically that set out in Article 6(1) Directive 95
[52] *Id* Article 10 & 11(1)
[53] *Id* Article 12
[54] *Id* Article 21

force in the third country in question and the professional rules and security measures which are complied with in that country." It seems clear that this provision is in place due to precisely the same fears expressed in this article, that being that certain countries lack the institutional strength to provide adequate protection from abuse of one's personal data and that transfer of such data to such countries produces unacceptable risk of such abuse.

Article 25 (6) of Directive 95 provides for the Commission to make a finding on whether a country ensures an adequate level of protection by reason of its domestic law or its international commitments with respect to "the protection of the private lives and basic freedoms and rights of individuals." The procedure that is in place for the positive recognition of a third country is a stringent one. A proposal is first required by the Commission, which is then subject to an opinion of the group of the national data protection commissioners[55]. An opinion of the management committee must then be delivered by a qualified majority of EU Member States and a thirty day right of scrutiny is provided to the European Parliament to examine the Commission's findings. The Parliament may then issue a recommendation to be adopted by the College of Commissioners if appropriate.

The Commission has so far only recognized a small number of countries, as providing protection at a level of adequacy for information to flow from Member States to these destination countries without further safeguard, which include Argentina, Switzerland, Canada, The Isle of Man and Guernsey. With respect to the United States the Commission has recognized such level of protection only for specific purposes, those being the US Department of Commerce's Safe Harbor Privacy Principles[56], and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection[57].

An examination of the recorded Commission decisions illustrate the caution that is taken by it and the other relevant EU institutions under the Directive when examining whether a country provides sufficient legal protection before personal data can flow to it. In the Commission decision relating to Switzerland[58] the various legal

[55] Article 29 of Directive 95
[56] Commission Decision 2000/520/EC of 26.7.2000 - O. J. L 215/7 of 25.8.2000
[57] Commission Decision of 14 May on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection
[58] Commission Decision 2000/518/EC of 26 July 2000

mechanisms for protecting an individuals right to privacy are examined in detail. The decision[59] refers to the Swiss Federal Constitution and protections afforded to one's privacy and protections against the misuse of personal data contained within that Constitution. It discusses at the same paragraph the body of case law developed by the Swiss Federal Court relating to the processing of personal data. The decision, in concluding that Swiss law provides adequate protection, makes reference[60] to the Swiss Data Protection Act[61] that applies to federal bodies and the private sector and which relates to among other things the transfer of data to foreign countries. Also examined is legislation adopted by the various Swiss cantons on data protection in areas for which they have jurisdiction such as education, police and direct cantonal taxes. After referring to Switzerland's ratification of the Council of Europe Convention 108 (3) referred to earlier in this paper, the decision states more generally that the:

> *"legal standards applicable in Switzerland cover all the basic principles necessary for an adequate level of protection for natural persons, even if exceptions and limitations are also provided for in order to safeguard important public interests. The application of these standards is guaranteed by judicial remedy and by independent supervision carried out by the authorities, such as the Federal Commissioner invested with powers of investigation and intervention. Furthermore, the provisions of Swiss law regarding civil liability apply in the event of unlawful processing which is prejudicial to the persons concerned."*[62]

If such an examination of the adequacy of legal standards and protections was to be made of many countries that European Member States have entered into TIEAs with, it is highly unlikely that a favorable decision would be reached by the Commission. Evidence of this may lie in the fact that so few countries been granted the status of providing adequate protection. While it is true that TIEAs contain confidentiality or secrecy clauses, which will be discussed in more detail later in this paper, it seems that countries within Europe, and the United Sates for that matter are increasingly entering into these agreements with countries that may be unable to

[59] At paragraph (6)
[60] At paragraph (7)
[61] 1993
[62] At paragraph (10)

guarantee adherence to such clauses. Additionally, the TIEAs themselves contain no mechanism that assesses a countries ability to adhere to such clauses, nor do they contain any mechanisms that seek to protect the data subject in the case of non-compliance with these clauses. The question must be asked whether, when balancing the individual's right to informational privacy and data protection against the important public interest of protecting against the loss of taxation revenue in countries unable to guarantee adequate protection, should the latter prevail?

Article 26 of Directive 95 provides for derogations from the Article 25 provisions relating to transfer of personal data to third countries. Article 25 (1) provides that:

> *"Member states shall provide that a transfer or set of transfer data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:*
>
> *...*
>
> *(e) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;"*

As stated earlier in this paper the importance of the public interest with respect to allowing transfer of personal data to countries with poor governance records or countries which do not ensure an adequate level of protection is questionable. The major focus of OECD countries in their push for TIEAs was to address the issue of tax revenues lost to IFC's and tax havens. As also earlier discussed, countries with poor governance and who are subsequently unable to ensure an adequate level of protection to an individuals personal data almost never qualify as IFC's or tax havens. In fact Andorra, which was identified in 2000 as meeting the OECD's tax haven criteria joined the small list of countries judged by the European Commission to provide adequate level of protection for personal data transferred from the European Union[63]. The level of tax revenue lost to governments from citizens in countries unable to provide adequate protection and hence the importance of the public interest when balanced against the individuals right to personal privacy must be called in to question.

Article 26 (2) of the Directive sets out the procedure whereby a Member state may:

[63] Commission Decision 1731 of 30 June 2003 - OJ L 168, 5.7.2003

"authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses."

An argument could be put forward that clauses contained within TIEAs relating to confidentiality and secrecy adequately fulfill the requirements set out in Article 26(2) even though they are not subject to the procedure set out in Article 31(2) which Article 26(3) refers to when providing for the ability of a Member state or the Commission to object to any derogation taken under Article 26(2). Such an argument would need to consider the clauses set out in the TIEAs that relate to confidentiality and other protective measures, an exercise that will take place later in this paper. First it is useful to examine cases in which Article 26(2) has been invoked and the detail of the safeguards and contractual clauses found to provide adequate protection.

One such example is the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) 2007. The European Council's decision [64] to enter into this Agreement extended an earlier short-term agreement, which followed an initial decision by the Commission[65]. That decision by the Commission was one regarding the adequate protection of personal data contained in the passenger name records of air passengers transferred to the United States' Bureau of Customs and Border Protection (CBP). Prior to the Commission reaching its Decision, the Commission and the US Department of Homeland Security (DHS) spent a year negotiating, which resulted in less personal data from the passenger name records of airlines being collected by US authorities, those records being kept for a shorter period and being used for more limited purposes, notably for the purposes of fighting against terrorism[66].

[64] 2007/551/CFSP/JHA
of 23 July 2007
[65] Commission Decision 2004/535/EC of 14 May 2004
[66] Europa Press Release IP/04/650 of 17 May 2009

Within the Commission's Decision[67] the Commission makes reference to the purposes of the relevant United States legislation, that being the enhancement of security and the conditions in which persons may enter and leave the country. In the same paragraph it states:

> *"The United States is a democratic country, governed by the rule of law and with a strong civil liberties tradition. The legitimacy of its law-making process and strength and independence of its judiciary are not in question. Press freedom is a further strong guarantee against the abuse of civil liberties."*

In the following paragraph of the Decision[68] the Commission outlines the European Community's commitment to fighting terrorism "within the limits imposed by community law." It states that community law must strike a balance between security concerns and privacy concerns and sites Article 13 of Directive 95 that enables Member states to restrict the scope of the Directive where it is necessary to do so for "reasons of national security, defense, public security and the prevention, investigation, detection and prosecution of criminal offences."

The Decision then goes on to outline in significant detail the conditions in which the CBP of the DHS will operate under the Agreement in order to fulfill the Community's privacy protection requirements. These are also given by way of undertakings that are annexed to the decision. The Decision highlights[69] the fact that all the statements in the Undertakings "will be, or have already been, incorporated in statutes, regulations, directives or other policy instruments in the United States and will thus have varying degrees of legal effect." It also points to the fact that:

> *"The Undertakings will be published in full in the Federal Register under the authority of the DHS. As such, they represent a serious and well considered political commitment on the part of the DHS and their compliance will be subject to joint review by the United States and the Community"* and that *"Non-compliance could be challenged as appropriate through legal, administrative and political channels and, if persistent, would lead to the suspension of the effects of this Decision."*

Other examples that show the depth of consideration and care taken before reaching the Decision are details of time and purpose limitations for the stored data,

[67] At paragraph (7)
[68] at paragraph (8)
[69] at paragraph (13)

conditions in which data can be forwarded on to other government agencies and the details of the workings of a DHS Privacy Office and it's Chief Privacy Offer. With respect to that Office the Commission states[70];

> *"CBP's respect for privacy in general will be under the scrutiny of the DHS's Chief Privacy Officer, who is an official of the DHS but has a large measure of organisational autonomy and must report annually to Congress. Persons whose PNR data has been transferred may address complaints to CBP, or if unresolved, to the DHS Chief Privacy Officer, directly or through data protection authorities in Member States. The DHS Privacy Office will address, on an expedited basis, complaints referred to it by data protection authorities in Member States on behalf of residents of the Community, if the resident believes his or her complaint has not been satisfactorily dealt with by CBP or the DHS Privacy Office. Compliance with the Undertakings will be the subject of annual joint review to be conducted by CBP, in conjunction with DHS, and a Commission-led team."*

The question must be raised that if such a cautious and thorough approach is taken by the Community in exercising the balance between security concerns and privacy concerns under Directive 95 with a country containing the level of governmental effectiveness, political stability, regulatory quality, rule of law and control of corruption[71] as the United States, how can the approach that is taken with respect to the transfer of personal data under TIEAs with countries that include Liberia be justified, due to concerns over tax avoidance?

Some answers may lie in a recent Communication from the Commission to the European Parliament, The Council and The Economic and Social Committee and The Committee Of The Regions entitled "A Comprehensive Approach on Personal Data Protection in The European Union[72]". The Communication acknowledges the significant changes brought about by rapid technological development and globalization and subsequently the new challenges for the protection of personal data. According to the Communication new technologies have resulted in methods of collecting personal data becoming increasingly elaborate and less easily detectable. In this context the Commission states that;

---

[70] at paragraph (22)
[71] These are the World Bank Worldwide Governance Indicators
[72] Brussels, 4.11.2010COM(2010) 609 final

"Public authorities also use more and more personal data for various purposes, such as tracing individuals in the event of an outbreak of a communicable disease, for preventing and fighting terrorism and crime more effectively, to administer social security schemes or for taxation purposes, as part of their e-government applications etc.[73]*"*

The Communication is a result of questions raised as to whether the existing EU data protection legislation is equipped to deal with these new challenges. In order to address this question a conference, public consultation and series of studies were launched. The findings were that the core principles of Directive 95 are still valid but a number of issues were identified as needing revision, such issues being outlined in the Communication. One of the key objectives outlined in the Communication is "ensuring appropriate protection for individuals in all circumstances". The Communication re-emphasises the principle set out in Directive 95 that:

"The definition of 'personal data' aims at covering all information relating to an identified or identifiable person, either directly or indirectly. To determine whether a person is identifiable, account should be taken of 'all the means likely reasonably to be used either by the controller or by any other person to identify the said person'"[74]

It is noted that this flexibility was imparted upon the Directive by its drafters to include situations and developments affecting fundamental rights that at the time were not foreseeable. It could be that one such unforeseeable development was the increased political will to protect national taxation revenues by engaging in TIEAs, including with countries with poor governance records.

Another area that the Commission pledges to address in its Communication is that of data protection rules in the area of police and judicial cooperation in criminal matters. Whilst this is not directly applicable to the issues at hand in this paper, it may be of some relevance. The Communication states[75] that the Directive 95 applies to all personal data processing activities in member states in both the private and public sectors but not to areas that fall outside the scope of Community law such as police and judicial co-operation in judicial matters. In particular it sights a need to "strengthen the EU's stance in protecting the personal data of the individual in the

[73] *Id* at page 2-3
[74] *Id* at page 5
[75] *Id* page 13

context of all EU policies, including law enforcement and crime prevention." The Communication makes reference to an EU instrument for the protection of personal data in the areas of police and judicial cooperation in criminal matters which is the Framework Decision 2008/977/JHA[76](the Framework). The Commission notes that the Framework is an "important step forward in a field where common standards for data protection were very much needed. However, further work needs to be done."

Specific criticisms the Commission make of the Framework are that there is a too wide exception to the limited purpose provision, lack of provisions relating to different categories of data being distinguished in accordance with their degree of accuracy and reliability, lack of provisions relating to data being based on facts as distinguished from opinions and a lack of provisions regarding distinctions being made between different categories of data subjects (i.e. criminals, suspects, witnesses etc.). The relevance of these remarks by the Commission is the evidence of recognition that reform is needed in privacy protection in areas that may be deemed of the public interest and in the interests of the state. This is even the case for the area of police and judicial cooperation which is specifically exempt from the operation of Directive 95, as opposed to economic or taxation matters which only attracts the rights of Member states to restrict the scope of obligations and rights of certain provisions of Directive 95.

Another area that is addressed and earmarked for reform by the commission in its Communication is the rules for international data transfers[77]. The Communication states that the exact requirements for recognition of adequacy by the Commission are not specified in satisfactory detail in Directive 95. They also point out the fact that the Framework Decision relating to cooperation in police and judicial matters does not provide for a Commission decision on the adequacy of third country protection as in the Directive. If the Commission is calling for such a safeguard to be implemented with respect to such matters, it would seem logical that a similar safeguard would be in place when European citizens are having their personal data transferred internationally under TIEAs.

[76] Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).
[77] At page 15

The Communication in fact recognizes that the current Commission standard clauses for the transfer of personal data are not well designed for transfers between public administrations[78]. In its response[79] to the Communication the Society of Trust and Estate Practitioners (STEP) EU Committee agrees with this assessment and argues that data transfers between tax administrations should be an area of particular focus in this context. STEP also argues that the Commission's stated objective of providing consistency in its evaluation of the adequacy of data protection in third countries should be applied in the context of data exchange between tax authorities.

The Communication specifically addresses the issue of international agreements concluded by the EU and its member states[80]and points out that they regularly require the inclusion of data protection principles and provisions. According to the Commission "this may result in varying texts with inconsistent provisions and rights, and thus open to divergent interpretations, to the detriment of the data subject." The Communication announces that the Commission will work on core elements for personal data protection in agreements between the Union and third countries for law enforcement purposes. In its submission STEP quite reasonably argues that TIEAs should be included in the Commission's work on defining core elements for data protection and that they could be used for all types of international agreements.

In that response STEP also identifies its concerns with the governance records of certain countries that have signed TIEAs to date and notes that the OECD has signaled its intentions to increase the tax information exchange network to more developing countries. While it quite rightly concedes that not all developing countries have weak governance and that TIEAs involving developing countries could play a useful role in deterring tax evasion, it states that for data to be shared with these or any country, tests must be applied that evaluate a country's quality of governance, freedom from corruption, security, stability and respect for law and human rights. In particular it highlights Liberia as a country that has signed TIEAs with a number of European countries that does or should not pass these tests. According to the World Bank indicators, Liberia is in the bottom 50 nations in the world in terms of quality of governance.

---

[78] At page 16
[79] European Commission Consultation: 'A comprehensive approach on personal data protection in the European Union', STEP Response of 11/1/2011
[80] *Supra* note 64

In its response to the Communication STEP highlights an example of problems that can arise when sharing information with governments that have poor governance records. This example is a recent UK court case[81] involving the Zimbabwean Government. In that case under the requirements of UK anti-money laundering legislation a bank was forced to take measures included blocking the requested transfers of the applicant due to suspicions that they involved funds that were criminal property. The transfers were intended for receipt in Zimbabwe and upon learning that they could not be fulfilled due to the suspicions (which in the end turned out to be unfounded) and the operation of the UK legislation, the Zimbabwean government froze and then seized the applicant's Zimbabwean assets resulting in losses of over $300m. This case illustrates the dangers that can occur when sensitive financial information is in the hands of governments with poor governance records.

The World Bank Worldwide Governance Indicators rate a country's percentile rank in 6 different categories. Those categories are voice and accountability, political stability, government effectiveness, regulatory quality, rule of law and control of corruption. Countries that have signed TIEAs with either the US, EU Member states or both include countries in the lowest 0 to 25th percentile in at least two of the categories. Examples of such countries include Liberia, Guatemala, Nigeria, The Philippines and Kenya. There are also many countries in the bottom 50th percentile, those countries including Colombia, Macedonia, Georgia, Indonesia, Jamaica, Vanuatu and Panama, Mexico and China.

4. A CLOSER LOOK AT TIEAs

In light of the fact that TIEAs are increasingly being concluded with countries that have poor governance records it is prudent to take a closer look at both the type of information that is transferred internationally under TIEAs, the circumstances under which it is transferred and the measures in place to ensure the information's adequate protection.

The creation and recent proliferation of TIEAs has been driven by the OECD as part of its objective to implement international tax standards[82]. In 1998 a report was issued by the OECD entitled "Harmful Tax Competition: An Emerging Global Issue".

[81] Shah and another v HSBC Private Bank (UK) Ltd, 4 February 2010
[82] Overview Of The OECD's Work On Countering International Tax Evasion, A Background Brief, Org. For Econ. Cooperation & Dev., 2 2, Feb. 18 (2011)

The report described the features of tax havens and the standards that were in place concerning transparency and information exchange. In 2000 the OECD drafted a blacklist of thirty-five tax havens that it identified as committing harmful tax practices and against which it would apply defensive measures[83]. According to the OECD Overview, between 2000 and 2002 it worked with the listed tax havens to "secure their commitment to implement the OECD's standards". In 2002 the OECD, working with forty-one non-OECD countries published the Model Agreement on Exchange of Information on Tax Matters (the Model Agreement). The Model Agreement is not binding though the OECD encourages countries to draft TIEAs based on this model[84]. The OECD Progress Report of 2010 states that all countries surveyed by the Global Forum have now committed to the internationally agreed tax standard[85]. As has been stated earlier in this paper the amount of TIEAs concluded in recent times has increased significantly[86]. In 2007 there were twelve TIEAs concluded compared to twenty-three in 2008 and one hundred and ninety-nine in 2009[87].

A. Scope of information exchange

In its Manual on the "Implementation of Exchange of Information Provisions For Tax Purposes (the OECD Manual)[88]" the OECD sites Article 26 of the Model Convention on Income and Capital (Model Convention) and Article 1 of the Model Agreement, which envisage information exchange to "the widest possible extent". It refers to the fact that under the Models "fishing expeditions" are not permitted in that information requests must have a connection to "an open enquiry or investigation". A balancing test standard of foreseeable relevance is set out concerning these two competing considerations. The commentary contained in the Model Agreement[89] is vague as to the actual standard of the foreseeable relevance test. The commentary states:

---

[83] *Id*
[84] *Id*
[85] *Id* at 16
[86] Keen, B, M. & Ligthart, J, E. "Information Sharing and International Taxation: A Primer" *International Tax and Public Finance* 13:1 (2006)
[87] *supra* note 84, at annex II, 13.
[88] Org. for Econ. Cooperation & Dev., Comm, "On Fiscal Affairs, Manual on the Implementation of Exchange of Information Provisions For Tax Purposes," Module 8 on Scope of Exchange of Information 11 1-4 (2006)
[89] Article 1 paragraphs (2) & (3) of the Commentary

"The standard of foreseeable relevance is intended to provide for exchange of information in tax matters to the widest possible extent and, at the same time, to clarify that Contracting Parties are not at liberty to engage in fishing expeditions or to request information that is unlikely to be relevant to the tax affairs of a given taxpayer."

It is difficult to see how such a test of foreseeability could be applied or enforced without judicial remedies in place to conclude whether the standard has been met and without a body of case law to serve as further guidance as to how the test should be applied. Of particular concern is the use of the word "unlikely" which is also used in the Joint Council Of Europe/OECD Convention On Mutual Administrative Assistance In Tax Matters that provides that "Information which is unlikely to be relevant to these purposes shall not be exchanged under this Convention[90]." This would seem to indicate a burden on the party receiving the request for the information to show it was in fact "unlikely to be relevant" should it ever wish to object based on the grounds that it believed the other party was undertaking a fishing expedition.

The Model Agreement does however set out the kind of information that a requesting authority should provide when requesting information to "show foreseeable relevance" under Article 5 of the Model Agreement. Only Article 5 (c) however, which calls for the tax purpose for which the information "is sought to be disclosed," seems to go directly to foreseeable relevance. The remainder of the required information merely describes the information sought, states where the requesting authorities believe it to be and why they can't obtain it within their own jurisdiction. It would seem that for a fishing expedition to occur a tax authority would need only to frame a credible tax purpose for which the information is sought. The final sentence of the first paragraph relating to the foreseeable relevance test is as follows and does little to ease the fear that a country would be able to indeed undertake a fishing expedition if it so wished; "Where a country fails to provide important pieces of information identified on this checklist, a requested competent authority may be led to believe that the request is a fishing expedition."

[90] Section 1; Article 4(1)(b).

As worrying is the volume of personal information that can be exchanged. According to Dean [91]the system of TIEAs has created a market in the form of a barter system where governments trade "bulk taxpayer information". He notes that with respect to individuals and businesses engaged in cross-border activities this creates "significant" privacy concerns, siting the fact that "The standard OECD electronic information exchange format allows for as many as 104 items of information about each taxpayer and his or her income[92]". Dean states that the volume of information about private parties exchanged between governments under TIE is "immense" and that by compiling so much "potentially sensitive" information the system works "too well".

The technological advances that have allowed for increased TIE may also create imbalances between the ability of developed and developing countries to ensure adequate protection of transferred data. Databases and technology networks are now used to transfer tax information internationally and steps need to be taken to create safeguards surrounding these transfers. It may be difficult however for governments in some developing countries with relatively meager technological and human resources to create and implement these required safeguards[93]. There is evidence of developing countries having difficulties with implementing IT systems in other areas such as customs[94]and there may be reason to believe that similar difficulties will arise with respect to information exchanged under TIEAs, which could have implications for a country's ability to ensure adequate safeguards.

B. Exchange of information on request

Article 26 of the Model Convention provides that broad information exchange can take place and does not limit the way in which it can take place[95]. The main forms of information exchange are on request, automatic and spontaneous. While the Model Agreement only applies to information exchange on request parties are free to

[91] Dean A, "The Incomplete Global Market for Tax Information", *Boston College Law Review,* Vol. 49, Issue. 3 N. 3, (2008)
[92] *Id* at 609.
[93] Cockfield *supra* note 4 at 30
[94] Jenkins, P, G. "Information Technology and Innovation in Tax Administration", *Information Technology and Innovation in Tax Administration The Netherlands: Kluwer Law International,* 7 (1996)
[95] OECD Manual *Supra* note 73 at 6

expand their own agreements to include automatic and spontaneous exchange[96]. Information on request is subject to the conditions set out above relating to the foreseeable relevance test. The Model Agreement contains a clause[97], as adopted in the agreement for example between the UK and Liberia, which states that "information shall be exchanged without regard to whether the conduct being investigated would constitute a crime under the laws of the requested Party if such conduct occurred in the requested Party." This clause is clearly of concern when considering that governments with good governance records may be assisting in the prosecution of crimes in countries with poor governance records for crimes that are not considered as such in their own country.

Article 5(4) of the Model Agreement provides that requested parties must have the authority to provide information including information held by banks and other financial institutions and information regarding the ownership of companies, trusts, partnerships and foundations.

C. Automatic information exchange

Information exchanged on an automatic basis is usually multiple information of the same category consisting of sources of income such as interest, dividends, royalties and pensions[98]. The information is transferred on a regular basis by the payer to the sending country and is then transferred to the other party under the agreement. Furthermore the foreign source tax information in digital form can be input directly into the receiving country's tax database and automatically matched against income reported by the taxpayer. This method, which is advocated in the OECD Manual as the most efficient method, has most likely led to an increase in bulk automatic exchange between governments[99].

This type of transfer is clearly not requested by a state due to any form of suspicion or as any part of investigation by a requesting state. In privacy legislation such as Directive 95 there are numerous provisions which provide for the data subjects right of access to that data[100] and the data subject's right to object[101]to the

[96] *Id*
[97] Article 5(1)
[98] OECD Manual *Supra* note 73 at 7
[99] Keen & Litghart, *supra* note 87 at 100.
[100] See Article 12 of Directive 95
[101] *Id* Article 14

processing of that data. Article 12 of the Directive is subject to exemptions and restrictions, however Article 15, which provides a right to object, is not[102]. Neither the Model Convention or Agreement contain provisions extending such rights to individuals whose information is exchanged under TIEAs, even in cases where information is not exchanged for the purposes of an investigation, civil or criminal, where an argument could be made that investigations would be impeded by providing access of that information to the data holder. The commentary on Article 8 of The Model Convention dealing with confidentiality of information refers to the fact that information "may be disclosed only to persons and authorities involved in the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to taxes covered by the Agreement". It states that this means the information may be provided to the taxpayer but that this is only "permitted" and not "required".

D. Spontaneous information exchange

The third type of transfer is the spontaneous exchange of information. This occurs when one contracting country passes on information to the other in the course of administering its own tax laws when it believes that such information will be of relevance to the foreign tax administration[103]. Whilst protective measures need to be taken for this type of exchange, above and beyond what is currently in place, this type of exchange is less concerning in terms of privacy rights violations than the two previously discussed. A sovereign nation is not compelled to transfer the information and is obligated to do so only in the event it feels that not transferring the information will result in the other party suffering a tax loss[104].

Whilst the Model Convention imposes the obligation to transfer the information if there is a belief that the tax revenue of the other party is jeapoardised, in reality a nation could choose to exercise discretion based on the current governance situation in the other party. For example if a political coup had recently taken place in a country with poor political stability, a country may not wish to transfer information to another party due to increased risks of privacy rights being violated as a result. Under information on request or automatic exchange of information they could only

[102] *Id* Article 13
[103] OECD Manual *supra* note 73 at 7
[104] Model Convention Article 7(1)

exercise this choice by termination of the agreement, which only becomes effective six months after the receipt of the notice of termination[105]. It may be that in such a case a state party would be able invoke Article 7(4) of the Model Agreement that allows a party to refuse a request for information on the grounds that it would be "contrary to public policy". However when looking to the commentary on Article 7(4) contained within the Model Agreement difficulties with this become apparent. It is stated that the exception can only be invoked in "extreme cases". Whilst the commentary does provide the example of a tax investigation in the requesting country being motivated by political or racial persecution it would seem that this would envisage the requested party being aware of that motivation at the time of a specific request. If a situation like one described above were to arise where a sudden change in the governance situation of an unstable country led to a fear for the data protection capabilities in general of the administration in that country, it unclear whether a state party would be able to invoke the refusal of a request provision of the Model Agreement.

E. The confidentiality clause

Article 8 of the Model Agreement is as follows:

"Any information received by a Contracting Party under this Agreement shall be treated as confidential and may be disclosed only to persons or authorities (including courts and administrative bodies) in the jurisdiction of the Contracting Party concerned with the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, the taxes covered by this Agreement. Such persons or authorities shall use such information only for such purposes. They may disclose the information in public court proceedings or in judicial decisions. The information may not be disclosed to any other person or entity or authority or any other jurisdiction without the express written consent of the competent authority of the requested Party."

It is the sole reference to confidentiality or the safeguarding of privacy in the Model Agreement. What is glaringly absent is any further protective mechanisms to oversee or enforce compliance which the clause which amounts too little more than an

[105] Model Agreement Article 16(2)

undertaking. As stated previously in this paper, for countries with trusted and established institutions, low levels of corruption and political stability, such an undertaking could be taken at face value, not withstanding the fact that the situation in that country could then change. With countries that are not able to instill such levels of trust, the value of such a clause is called into question. The commentary on Article 8 provides that "Exchange of information for tax matters must always be coupled with stringent safeguards to ensure that the information is used only for the purposes specified in Article 1 of the Agreement" and that "The Contracting Parties must have such safeguards in place". There is however no elaboration on what these stringent safeguards must entail. The commentary also refers to the fact that information "may be disclosed only to persons and authorities involved in the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to taxes covered by the Agreement". It states that this means the information may be provided to the taxpayer but that this is only permitted and not required.

F. Disclosure to oversight bodies

Article 26 of the Convention at Paragraph 2 allows for the transfer of individual's tax information to oversight bodies, such as a legislative committee[106]. In a report (the UN Report) considering revisions of Article 26 of the Model Convention that occurred in 2005, a UN Committee of Experts on International Cooperation in Tax Matters (UN Committee) considered whether to make changes to the United Nations Model Double Taxation Convention[107]along the same lines as those made to the OECD Model Convention. One area that came under consideration for the UN Committee was whether to adopt in their own Convention the changes made to the OECD Model Convention that introduced the permission of disclosure of personal tax information to oversight bodies.

[106] United Nations Economic and Social Committee, Committee of Experts on International Cooperation in Tax Matters, "Report of the Ad Hoc Group of Experts Meeting on Exchange of Information (Revision of Article 26 of the United Nations Model Double Taxation Convention between Developed and Developing Countries)"(2005)

[107] United Nations Model Double Taxation Convention between Developed Developing Countries

The change was requested by the United States to allow for the disclosure of information to congressional committees involved in tax matters[108]. The extension of Article 26 of the Model Convention to include transfer of information to oversight bodies raises some troubling issues, which are well expressed in the UN Report. Participants in that report expressed concern that oversight bodies in many developing countries "would not view tax information the way it is expected to be treated by the tax authorities[109]" and that "individuals in these bodies would be likely to leak the information for political or other purposes." In expressing its concerns the UN Committee notes its understanding of the OECD position but that it feels that it carries significant risks. The Committee states that it does not feel oversight bodies should be allowed to receive information obtained through TIEAs unless they are subject to the same controls as tax authorities.

Notably the Committee found that in addition to the oversight bodies being subject to the same controls as tax authorities "the parties need to be assured that those controls will be effective." The end decision of the Committee was one not to endorse the OECD proposal "Given the uncertainty that such conditions would be met in the general case." This decision of the Committee, while relating only to the transfer of information obtained under TIEAs to oversight bodies, highlights the difference between controls being in place and those controls being effective. With respect to certain developing countries the UN Committee could not be convinced that effective controls were in place with regards to oversight bodies, which are "likely" to leak information. If these fears exist with respect to oversight bodies it appears questionable that such dangers would not also be present with the tax authorities in certain jurisdictions. It is for precisely these reasons that further mechanisms need to be put in place to further protect taxpayer privacy under TIEAs. Some recommendations for such mechanism are discussed below.

5. RECOMMENDATIONS

The most simple and immediate form of protection against the possible breach of taxpayer privacy and misuse of taxpayer information under TIEAs would be for governments to exercise the necessary prudence when deciding with which countries they should enter into such agreements. This would require an assessment by the

[108] *Supra* note 106.
[109] *Id* at 4.

relevant parliamentary or congressional body as to the suitability of the proposed agreement partner based on available information such as, for example, the World Bank Governance Indicators. In the immediate future this seems to be unlikely to happen as the trend towards signing TIEAs with developing countries, some of which contain poor governance records, is an upwards one, driven by the OECDs drive for the expansion of tax information exchange. In any event, even if the politicians of all countries were to suddenly start debating whether each new proposed TIEA should be signed based on the adequacy of the other party's data protection laws and governance records, such a change in circumstances would provide only a temporary solution.

A party to a TIEA signed today adjudged to provide adequate protection could very quickly turn into one that does not provide such protection. For example, a new government could repeal data privacy legislation or a protest movement could suddenly become the victim of a vicious crackdown in which information exchanged under TIEAs was used to locate and persecute members of the movement. As previously stated under the OECD Model Agreement, TIEAs can only be terminated six months after the serving of the notice of termination, leaving tax-payers at risk to the types of situations described above for an unacceptable period of time. What is more, the provisions under the Model Agreement relating to refusal of requests for information do not seem to adequately provide signatory governments with the tools to protect against such situations.

A. Amending legislation

This paper has argued that TIEAs, particularly the vast majority that are based upon the OECD Model Agreement, create a danger with respect to the privacy rights of taxpayers. This is especially so with respect to TIEAs that are concluded with a number of countries with poor governance records. A simple answer to this problem could be to not enter into such agreements unless the governments of prospective parties passed some kind of test regarding strength of governance and in particular, ability to adequately protect the privacy of taxpayer information that is transferred under such agreements.

As discussed earlier in this paper Blum[110]suggests an amendment to Section 6103(k)(4) of the IRC, the section that permits the transfer of personal tax data from the United States under information exchange agreements. She states that the amendment should restrict the transfer of tax information to countries that can provide assurances that the information will be used for the purposes intended. A model to be used as a template is that of Singapore. Singapore, when amending Chapter 134 of its Income Tax Act[111]in 2009 to "enhance international cooperation on information exchange[112]" included provisions[113]which require the Comptroller, when seeking certain types of information[114]for transmission to partners under TIEAs, to apply to the High Court of Singapore for an order releasing the information. This application must be supported by a written authorization from the Attorney General. The High Court may not issue the order unless it is satisfied that the transfer is neither contrary to public policy nor will it authorize the disclosure of information protected by legal privilege.

This is a measure that would prove valuable in the protection of taxpayer's privacy rights and could be included in the national legislation enabling TIEAs in all countries that value the protection of informational privacy. It could be expanded to include a Court order being necessary for all information transferred under TIEAs. The requirement that the transfer not be contrary to public policy could conceivably capture a consideration as to whether the information will be afforded adequate protection in the receiving country. Preferable however would be a more explicit requirement that the transfer will not endanger the privacy rights of the data subject.

Concerns could arise that this process will result in delays that will serve to jeopardize the efficient function of TIEAs and their purpose of protecting national tax revenue. For this reason it may be that the High Court or national equivalent in other countries is not the appropriate jurisdiction to hear such applications. A more expedient and efficient forum such as an administrative tax tribunal may be preferable. If the tribunal or court in question had recently judged a country to provide

---

110 *Supra* note 10 at 624
111 Cap 134, (2008 Rev Ed)
112 Income Tax (Amendment)(Exchange of Information) Bill 2009
113 105I-105M
114 Where the information sought is in the possession of to whom either Section 47 of the Banking Act (Cap 19, 2003 Rev Ed) and Section 49 of the Trust Companies Act (Cap 336, 2006 Rev Ed) applies.

adequate protection then applications could be processed almost automatically until new information was presented that altered the situation.

With respect to Europe it has previously been stated in this paper that the Commission has proposed that it will work on core elements for personal data protection in agreements between the Union and third countries for law enforcement purposes. It also noted that there was a deficiency in the Framework Decision relating to cooperation in police and judicial matters in that it does not provide for a Commission decision as to the adequacy of data protection in third countries as Directive 95 does. A similar framework could be designed for international tax information exchange with a mechanism in place that requires a decision from the Commission, as set out in Directive 95. That decision could be one that allows for automatic transfer of tax information to non Member states that have been judged by the Commission to provide adequate protection in terms of strength of data privacy law, the strength of institutions and other considerations that are set out in the Commission decisions thus far taken pursuant to Directive 95.

B. A Multi-Lateral Agreement

The OECD Model Agreement also refers to the possibility of a multi-lateral TIEA. Cockfield identifies certain dangers associated with taxpayer privacy interests under a multi-lateral TIEA[115]. These include the fact that a larger network of information sharers increases the risk that taxpayer information will be used improperly or leaked by a third party government as more parties to the agreement will likely be provided with access. Governments may find it difficult to remain accountable and responsible for transferred information that is transferred to multiple parties. Nevertheless Cockfield advocates such an agreement provided it includes additional safeguards and protections of taxpayer rights that do not already exist under the bilateral agreements. The additional safeguards and protections he proposes are in the form of a Sample Multi Lateral Tax-Payer Bill of Rights (Sample Bill of Rights), which is attached as an appendix to his paper. In drafting his Sample Bill of Rights Cockfield draws on a number of existing legal instruments including Directive 95,

[115] *Cockfield* note 4 at 21.

which acts as a guide for "the collection, use and disclosure of personal information by governments and industry".

For a Multi-lateral TIEA to function in a manner that protects taxpayer privacy, a body or committee of some form should be created in order to evaluate which signatory countries provide adequate safeguards. Those which do not could be subject to the refusal of information requests by other parties to the agreement on the grounds that adequate protections are not in place and that a breach of the data subjects privacy rights as set out in the Sample Bill of Rights is likely to occur as a result of the transfer. Examples of provisions of the Sample Bill of Rights relating specifically to the misuse of illegal transfer of tax information that may be called upon to refuse a request to transfer include;

> *"**2. Taxpayer has the right to privacy and confidentiality.***
> *A taxpayer can expect foreign tax authorities to protect the privacy and confidentiality of their tax information. This information will be used only for purposes allowed by law. Only those persons who are authorized by law and who require the information to administer programs and legislation have the right to access a taxpayer's personal and financial information.*
> *...*
> ***8. Taxpayer has the right to expect the tax authority to be accountable.***
> *A taxpayer has the right to expect tax authorities to be accountable for what they do. When a tax authority makes a decision about a taxpayer's affairs, the authority will explain that decision and inform the taxpayer about its rights and obligations in respect of that decision. If a tax authority transfers a taxpayer's information across a border, the original tax authority remains accountable for the treatment of this information even after it relinquishes control over the information. A taxpayer has the right to challenge tax information relating to the taxpayer and, if the challenge is successful, to have the information amended or erased.*
> *...*
> ***13. Taxpayer has the right to have its tax information protected by reasonable security safeguards when it is transferred across borders.***
> *Taxpayer information should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification.*

Drawing once more upon Directive 95 as a model, the proposed committee could be made up of independent expert representatives of the 30 OECD states as well as all other jurisdictions participating in the Global Forum on Transparency and Exchange of Information. This Committee, operating in a role similar to the European Commission when assessing adequacy of protection of third countries under Directive 95, would assess the data protection capabilities of each new signatory to the multi-lateral agreement. In addition it would respond to applications to have existing signatories struck off or re-instated to a register of countries providing adequate protection. The criteria for acceptance to the register would be compliance with the Tax-Payer Bill of Rights as well as other factors such as positioning on the World Bank Governance Indicators. Under Article 8 of the Sample Bill of Rights a taxpayer would have recourse to seek remedies under national courts for failures to comply with the Bill of Rights.

C. Carrots and Sticks

The question arises as to what motivating factors are present for a nation with inadequate protections to join the multi-lateral agreement, or if already a signatory, to comply with its requirements. With respect to 'sticks' the same negative motivating factors that pushed many nations into signing bilateral TIEAs could still be utilized. Once a party is a signatory to the multilateral agreement it will still need to comply with requests for information transfers should it be on the register of non-compliant countries, but will not be able to enforce its own requests for information.

Perhaps more important is the question of what positive motivating factors, or 'carrots' could be employed to encourage countries to join the multi-lateral agreement and as a result improve their privacy safeguards to the required level. One 'carrot' could be for residence countries to allocate part of any revenues derived from information sharing back to the host countries[116]. Other 'carrots' could include non-tax incentives provided on the basis of compliance with TIEAs (including the Bill of Rights) such as expanding trade and investment relations, offering places in universities and providing assistance with technology required for the successful implementation of TIEAs, including the safeguards necessary to protect private data

[116] Keen, M. and Lithgart, E, J. "Incentives and Information Exchange in International Taxation" (2006) 13 *Int'l Tax Pub. Fin.* 163 at 176

when such technology is implemented. It could be that such technology transfers are beneficial to the receiving country in areas other than tax information exchange, such as updated databases for customs.

7. CONCLUSION

This article has identified the rapidly increasing cross border exchange of taxpayer personal information under OECD instigated Tax Information Exchange Agreements. A myriad of national and regional privacy and data protection laws are in place to protect personal informational privacy such as constitutional and statutory protections in the US and the EU Data Protection Directive. The political push for tax information exchange has however seen many of these protective measures forgotten in the race to protect national tax revenue. While the desire for governments to protect their tax revenue is certainly a legitimate one and tax information exchange can certainly be helpful in achieving that aim, there is no reason why this can't be achieved in conjunction with the goal of maintaining and even improving international data privacy standards.

Unfortunately many, but not all, developing countries are unable to currently provide adequate protective measures to ensure security and privacy of an individual's information and data due to reasons such as poor governance, political instability and insufficient resources. There are a number of approaches that can be taken to ensure that this does not result in the breach of an individual's informational privacy rights. One is for governments to enact legislation that imposes a standard of data protection on its TIEA partners that must be met before transfers take place. Another is bringing these countries into the fold in the form of a multi-lateral framework that requires compliance with data protection principles and offers rewards for the adherence to such principles.

Bibliography

Blum, C. "Sharing Bank Deposit Information With Other Countries: Should Tax Compliance or Privacy Claims Prevail?" *Florida Law Review,* Vol. 6:6 (2004)

Cockfield, J A. "Protecting Taxpayer Privacy Rights under Enhanced Cross-border Tax Information Exchange: Toward a Multilateral Taxpayer Bill of Rights" *University of British Columbia Law Review*, Vol. 42, (2010)

Cate, F. "The EU Data Protection Directive, Information Privacy and the Public Interest", *Iowa Law Review,* 80 (1995)

Dhammika D & Hinse R J, "Why Do Countries Become Tax Havens?" NBER Working Paper No. 12802, (2009)

Desai, Mihir A., C. Fritz Foley, and James R. Hines Jr., Do tax havens divert economic activity?" *Economics Letters*, (2006), 90 (2), 219-224; Desai, Mihir A., C.

Elkin Koren, N & Birnhark, M, "Privacy in the digital Environment", *The Haifa Centre of Law and Technology Publication Series*, Publication No. 7 (2005).

European Commission, "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and The Committee of the Regions: A comprehensive approach on personal data protection in the European Union", Brussels COM 609 final (2010)

Foley, F & Hines Jr, J, R. "The demand for tax haven operations, *Journal of Public Economics*, 513-531 (2006)

Hines R J, "International Financial Centers and The World Economy", *STEP Report,* 11 (2009)

Jenkins, P, G. "Information Technology and Innovation in Tax Administration", *Information Technology and Innovation in Tax Administration The Netherlands: Kluwer Law International,* 7 (1996)

Keen, M. & Lithgart, E, J. "Information Sharing and International Taxation: A Primer" *International Tax and Public Finance* 13:1 (2006)

Keen, M. and Lithgart, E, J. "Incentives and Information Exchange in International Taxation" 13 *Int'l Tax Pub. Fin.* 163 (2006)

Lessig, L. "The Architecture of Privacy", *Van. J. Ent. L. & Prac*. 56 (1999)

Linder, M." Tax Glasnost for Millionaires: Peeking Behind the Veil of Ignorance Along the Publicity-Privacy Continuum," *N.Y.U. Rev. L. & Soc. Change* 951, 971 (1990/1991).

Miller, R, A. "The Assault on Privacy: Computers, Databanks, and Dossiers" *U. ILL. L.F* 154, 168 (1971)

Org. for Econ. Cooperation & Dev., Communication, "On Fiscal Affairs, Manual on the Implementation of Exchange of Information Provisions For Tax Purposes," Module 8 on Scope of Exchange of Information 11 1-4 (2006)

Org. For Econ. Cooperation & Dev "Overview of the OECD's Work On Countering International Tax Evasion, A Background Brief", 2 Feb. 18 (2011)

Posner, R. "The Economics of Justice", *Harvard University Press,* 234-35 (1983)

Posner R. A, "The Right of Privacy", *Georgia Law Review*, Vol. 12, No.3 (1978)

Richard W, R. "The Future of Money and Financial Privacy, in The Future of Financial Privacy-private choices versus political rules", *The Competitive Enterprise Institute,* ed. 126, 132 (2000).

Slemrod J, "Why Is Elvis on Burkina Faso Postage Stamps? Cross-Country Evidence on the Commercialization of State Sovereignty", *Journal of Empirical Legal Studies, Volume 5,* Issue 4, 683–712 (2008)

Slemrod J, 'Taxation and Big Brother: Information, Personalisation and Privacy in 21st Century Tax Policy', *Fiscal Studies*, vol. 27, no.

(2006).

Society of Trust and Estate Practitioners EU Committee "European Commission Consultation: 'A comprehensive approach on personal data protection in the European Union', STEP Response" (11/1/2011)

Swire, P, P. "Financial Privacy and The Theory of High-Tech Government Surveillance", 77 *Wash. U. L. Q.* 461, 470 (1999)

Turkington, R. C, "Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy" 10 *N. Ill. U. L. Rev*. 489 (1989-1990)

United Nations Economic and Social Committee, Committee of Experts on International Cooperation in Tax Matters, "Report of the Ad Hoc Group of Experts Meeting on Exchange of Information (Revision of Article 26 of the United Nations Model Double Taxation Convention between Developed and Developing Countries)"(2005)

Warren & Brandeis, "The Right to Privacy" *Harvard Law Review*, Vol. 5, No. 5, (1890)

Westin, A, F. "Privacy and Freedom", 25 *Wash. & Lee L. Rev* 166 (1967)