International Issues 6

Law enforcement efforts focusing only on domestic wire transfers would be of little utility, in view of the transnational nature of much money laundering.[1] Moreover, a screening system's best chance of success may be with international wires, where there are additional markers of suspiciousness, such as country of origin or receipt,[2] route through an offshore banking haven, or connection to an anomalous non-export related business.

As noted in previous chapters, the incoming wire transfer has become increasingly interesting to law enforcement, with the growing realization that money launderers find the United States a stable and attractive site for investment, particularly in comparison with countries undergoing political risk and currency upheavals.[3] But access to international wire transfers raises policy questions beyond those of monitoring domestic transfers. While U.S. law enforcement may currently subpoena international wire

[1] For instance, the American Express Bank International of Texas laundered funds through the Cayman Islands, ultimately paying a $32 million fine. New York *Times*, Nov. 22, 1994, p. A1(N), p. D2.

[2] Not every international wire transfer will be transparently international: a U.S. bank with foreign subsidiaries may number foreign accounts differently, thus what appears to be a domestic transfer to the U.S. bank may suffice to transfer funds to an account held by the foreign subsidiary.

[3] At the same time, there are substantial questions about the difficulty of detecting incoming money laundering wires in light of the fact that the money has already been laundered to the point where its owner is confident about returning or bringing the funds to the United States. Others believe that the domestic legs of an international funds transfer may themselves raise suspicions, as was observed in the Bank of Commerce and Credit International (BCCI) case, characterized by a churning of money through transfer after transfer.

transfer records held by U.S. banks,[4] information regarding the originator of the wire transfer may have already been lopped off or protected by the originating foreign bank. Foreign bank secrecy laws, which entail the possibility of criminal sanctions being brought against foreign banking officials responsible for revealing financial information about their customers, may be a significant impediment to tracing the flow of funds back to their source, as is the profit incentive informing bank secrecy laws in the first place.

The role of offshore banking havens in the legitimate and illegitimate economies of the United States and the world is discussed in this chapter. Offshort banking havens present a twofold problem for wire transfer screening systems. First, they undermine the utility of monitoring incoming wire transfers by the financial anonymity they can provide. Second, they compete with U.S.-based banks, undercutting the acceptability of monitoring to the banking community in the United States, particularly as monitoring may threaten the lucrative dominance of the dollar in international payment systems. The more scrutiny directed at customers of U.S. financial institutions, the more attractive offshore banking havens will become.

This chapter will also discuss data protection initiatives governing the transborder flow of information, generated by the European Union (EU), the Council of Europe, and the Organization for Economic Cooperation and Development (OECD). The unilateral monitoring of international wire transfers could damage international relations, particularly with close allies in Europe.[5] It could even imperil otherwise fruitful cooperation in the pursuit of money laundering among international law enforcement bodies.[6]

Finally, this chapter will look at the efforts of the United States in combating international money laundering, unilaterally and through multilateral and bilateral cooperation and agreements aimed at criminalizing money laundering, creating cash transaction records and gaining cooperation in the piercing of bank secrecy. The issue of access to international data becomes embroiled in the conflict between expanding notions of sovereignty and the effects of communications networks. One solution to this tension might be multilateral negotiations aimed at the control of money laundering by permitting law enforcement access while otherwise preserving a state's legitimate interest in bank secrecy and data protection. Bank haven countries, however, might be expected to resist such efforts.

ACCESS TO INTERNATIONAL WIRE TRANSFER INFORMATION

Foreign Bank Secrecy

Foreign bank secrecy laws do not curtail the ability of U.S. law enforcement to subpoena international wire transfer records held domestically (see box 6-1). Nevertheless, these laws and the ethos underlying them do present a potential impediment to obtaining comprehensive information on international wire transfer and following up on investigative leads. In general, bank secrecy laws prohibit banking officials from releasing confidential customer information to third parties outside the financial institution. Bank secrecy may be

[4] Under section 1515 of the Annunzio-Wylie Anti-Money Laundering Act of 1992, Treasury and the Federal Reserve Board may "request" from U.S. banks international funds transfer records required to be held by the wire transfer regulations. 12 U.S.C. 1829b(b)(3)(C). As the regulations only take effect on the first of January 1996, this "request" authority has not yet been tested.

[5] This conflict will become sharper with the promulgation of the final version of the European Union's (EU) Data Protection Directive (see text *infra*).

[6] Access to international wire transfers for U.S. law enforcement raises the question of whether the United States should risk interfering with the international flow of capital, with the unlikely but potentially dire effects of discouraging foreign direct investment in the United States. In addition, the United States has security interests in the use of the dollar-based payment system, since economic sanctions depend on blocking/freezing of assets held by or going through U.S. banks.

BOX 6-1: Nonspecific Subpoenas Targeting International Wire Transfers

Comity, or the voluntary deference of U.S. courts to foreign laws (for example, bank secrecy laws), complicates efforts at reaching records held offshore. In the 1980s, the U.S. Internal Revenue Service (IRS) served a "John Doe" or nonspecific, subpoena on several northern California banks, seeking records related to international funds transfers to certain tax haven countries. Although the Bank of America had cooperated and produced copies of wire transfer records held in the United States involving wire transfers to and from certain countries, in the early 1990s, the IRS sought to enforce the subpoena and obtain records relating to wire transfers held by a Bank of America subsidiary in Hong Kong. Hong Kong has a general commercial confidentiality statute, Protection of Trading Interests Act of 1980, criminalizing the disclosure of commercial information. A federal district court refused to require that Bank of America produce the records held abroad. *In re the Matter of Tax Liabilities :John Does*, No. C-88-0137 Misc (N.D. Cal., March 11, 1992) (Wieking, J.). The district court applied section 442 of the American Law Institute's *Restatement of the Law (Third) on the Foreign Relations of the United States*,[1] in finding that the subpoena was "generic in its terms and in its purpose. . . . [not] aris[ing] from an investigation of any particular alleged misconduct, nor does it seek evidence of particular identified transactions." *Ibid*., p. 15. Under section 442, these factors cut against enforcing the subpoena with respect to records held abroad, even though the vital U.S. interest in detecting tax evasion was implicated. The district court's ruling is the flip side of holding U.S. subsidiaries of foreign banks to the U.S. standard in producing records held in the United States; by the same token, U.S. banks doing business abroad will take on characteristics of the bank secrecy jurisdiction hosting them.

A salient point is confirmed by this case: apparently the Protection of Trading Interests Act did not bar the transmission of the wire transfers to the United States even though authorities in Hong Kong were on notice that the records would be scrutinized by U.S. government authorities. That aspect of the John Doe, or nonspecific, subpoena was upheld in Northern California, and had resulted in the disclosure of some 13,000 wire transfer records to the IRS as of March 1992, leading to 10 cases referred for criminal prosecution.

[1] Section 442 of the Restatement states that a court or agency should only issue a subpoena or summons upon consideration of the importance of the information sought; the degree of specificity of the request; the provenance of the information (in the United States or abroad); the availability of alternative means of gaining the information; the extent to which compliance with the summons would trench on the foreign nation's interest and the extent to which noncompliance would adversely affect U.S. interests.

SOURCE: Office of Technology Assessment, 1995.

a matter of common law, civil or penal law, or perhaps even a constitutional precept.[7] There are two kinds of bank secrecy laws—"blocking statutes" and true bank secrecy provisions such as Article 47 of the Swiss Confederation. The latter involve the legal requirement of confidentiality of information and impose civil or criminal penalties for unauthorized disclosure of customer informa-

[7] Article 18 of the Spanish constitution guarantees secrecy of communication and limits the use of personal information in order to protect personal privacy. This article would likely shelter financial data.

tion.[8] In the Bahamas, bank secrecy provisions penalize improper disclosure with the possibility of a two-year prison sentence.[9] Blocking statutes, on the other hand, do not establish a confidential relationship between customer and bank. They are invoked only when a foreign law enforcement agency attempts to access account records, may be waived only by the sovereign, and represent the efforts of states to resist extraterritorial application of another state's laws.[10]

Foreign bank secrecy and blocking laws affect investigations in the United States primarily through the judicial doctrine of "comity," or a U.S. court's "essentially voluntary deference to the acts of other governments, undertaken for the common good even though no transnational institution exists to exert any compulsion."[11] This doctrine usually arises when U.S. law enforcement seeks to enforce a subpoena directed at records held abroad in a bank secrecy jurisdiction. The basis for comity is the perception that a state should forbear from presenting the citizen of another sovereign with the alternative of violating either its laws (i.e., by refusing to obey a court order to present records) or the laws of the citizen's sovereign, specifically, foreign bank secrecy laws prohibiting the disclosure of bank records. But some U.S. courts have found that the national interests in stemming illegal drug trade are more vital than any foreign interest in bank secrecy (a factor in the balancing test of whether to impose contempt on a non-complying bank officer).[12] Other courts have been even less solicitous of comity concerns, finding merely that a willingness to do business in the United States fairly subjects a corporation to the relative rigor of U.S. criminal investigations.[13]

Again, bank secrecy is not necessarily an absolute barrier to law enforcement, particularly once an investigation has yielded strong evidence about criminal conduct of accountholders in bank secrecy jurisdictions. Bank secrecy jurisdictions have come to recognize that their laws may shelter narcotics traffickers and have begun cooperating with international law enforcement efforts. Switzer-

---

[8] The Swiss Federal Law on Banks and Savings Banks, article 47 provides in part:

Persons who disclose confidential information entrusted to them or which has come to their knowledge in their capacity as official, [or] employees [of banks]. . . shall be penalized by imprisonment not to exceed six months or a fine not to exceed SFr. 50,000.

Reprinted and translated in *Federal Law on Banks and Savings Banks* (Switzerland: Union Bank of Switzerland, 1990).

It is highly interesting to observe that in Swiss criminal cases, bankers may be obliged to testify and produce relevant documents, as reflected by clause 4 of Article 47—"Federal and cantonal regulations regarding the obligation to testify and to furnish information to government authorities shall also apply." *See also* Dunant, Olivier and Wassmer, Michele, "Swiss Bank Secrecy: Its Limits Under Swiss and International Laws," 20 *Case W. Res. J. Int'l L.* 541-575, pp. 549-550 (1988).

[9] Banks and Trust Companies Regulation Act of 1965, 1965 Bah. Acts No. 64, art 10, *as amended by* Banks and Trusts Companies Regulation (Amendment) Act, 1980, 1980 Bah. Acts No. 3.

[10] Many blocking statutes, designed to thwart foreign governments' access to records, were enacted in direct response to U.S. extraterritorial subpoenas. The Restatement of the Law of Foreign Relations of the United States (Third), at 442, note 4 (1987). As of 1986, some fifteen states had adopted legislation expressly designed to counter United States efforts to secure production of documents located outside the United States. *Id.* at 442, Reporters' Note 1. These countries include the United Kingdom and France.

Section 442 provides guidance to U.S. courts in their enforcing of subpoenas with international dimensions. Significantly, section 442(c) directs the court to take into account "the degree of specificity of the request" and "whether the information originated in the United States."

[11] 18 Wright, Miller & Cooper, *Federal Practice and Procedure*, 4473 (1981).

[12] *United States* v. *Bank of Nova Scotia (II)*, 740 F.2d 817, 827 (11th Cir. 1984), *cert. den'd*, 462 U.S. 1119 (1985); *United States* v. *First National Bank of Chicago*, 699 F.2d 341, 347 (7th Cir. 1983) (nonetheless overturning a district court's contempt order sanctioning defendant for failing to comply with a subpoena for records of alleged tax evaders).

[13] See, e.g., *In re Grand Jury Proceedings United States* v. *Field*, 532 F.2d 404, 410 (5th Cir.), *cert. den'd*, 429 U.S. 940 (1976).

land, for example, has signed a Mutual Legal Assistance Treaty (MLAT) with the United States,[14] ended anonymously held bank accounts and now requires the beneficial owner's name to appear on bank records.[15]

Even if the letter of bank secrecy laws does not impede the monitoring of international wire transfers, the ethos of confidentiality for a price works against the success of any monitoring proposal. Bank secrecy is lucrative both for the banks and their host countries. Hence, foreign bankers might be expected to strip away the history of a wire transfer before its ultimate transfer into the United States. These precursor wire transfers, while not necessary for completing the transfer and perhaps impossible to fit into existing wire transfer formats, are most interesting to U.S. law enforcement. Even if the United States were to refuse to permit domestic banks to process incoming wires that did not have names in the originator fields (as the U.S. Treasury Department's proposed 1989 wire transfer rules provided[16]), a bank could still please both sovereigns by inserting plausible yet false names in the originator field; accurate originator information is not necessary to the successful processing of the transaction.[17]

The Role of the International Offshore Bank in the World Economy

With the dramatic rise of international banking havens over the past 30 years, obscure island nations have surged to prominence in the international banking economy.[18] Legitimate businesses have long banked in and routed wire transfers through secrecy jurisdictions.[19] Banks book assets on behalf of their customers in offshore banking havens in part to avoid Federal Reserve requirements: slightly higher interest rates may be paid on customer funds held offshore, since the bank need not hold the reserve amount in a non-interest-bearing account with its district Federal Reserve Bank. Early newspaper accounts indicate that Barings Bank opened a special account in the Cayman Islands to cover margin calls for the futures trading of Nicholas Leeson, perhaps to skirt Bank of England regulations requiring notice when more than

---

[14] The U.S.-Switzerland Mutual Legal Assistance Treaty was successfully invoked as early as 1978, in the prosecution of Stanley Mark Rifkin, who fraudulently wire transferred money from a Los Angeles bank account to his Swiss bank account. James I.K. Napp, "Mutual Legal Assistance Treaties as a Way to Pierce Bank Secrecy," 20 *Case Western J. Int'l Law* 405-433, 405 (1988).

[15] Switzerland is a member of the Financial Action Task Force (to be described below) and has agreed on to the Forty Recommendations of FATF, including the prohibition on anonymous transactions.

[16] *Bank Secrecy Act Regulatory Applications to the Problem of Money Laundering Through International Payments*, 54 *Fed. Reg.* 45769, 45771 (Oct. 31, 1989)(requiring that all international wire transfers contain all known originator and beneficiary identifying information).

[17] One commentator cites several wire transfer experts stating that nonsense words could fill any mandatory "on-whose-behalf" field. Sarah Jane Hughes, "Policing Money Laundering Through Funds Transfers: A Critique of Regulation Under the Bank Secrecy Act," 67 *Indiana Law J.* (Winter 1992), 283-330, 296, n.77 and 305 (citations omitted).

[18] Vanuatu (in the South Pacific), Niau, Republic of Nauru, and St. Kitts, *inter alia*. See chapter 4, footnote 31 for a complete list. Long ago, Congress recognized the role that banking haven countries played in abetting tax evasion and other crimes. The 1970 Bank Secrecy Act requires that U.S. nationals file yearly Foreign Bank Account Reports with the Internal Revenue Service (IRS) detailing foreign accounts and transactions with foreign banks in excess of $5,000.

[19] Susan Roberts, "Fictitious Capital, Fictitious Spaces: the Geography of Offshore Financial Flows," in Stuart Carbridge, Nigel Thrift and Ron Martin (eds.), *Money, Power and Space* (Oxford, U.K.: Blackwell, 1994), pp. 91-115.

25 percent of a group's capital is transferred to a subsidiary.[20]

A former investigative counsel with the Senate Foreign Relations Committee, Jack Blum, notes that judging by its wire transfer traffic, the Cayman Islands represent the fifth largest banking economy in the world.[21] Blum and others have explored the role of offshore banking havens, arguing that the bank secrecy offered by these jurisdictions attracts either those seeking to avoid regulation and taxation or those whose source of funds is itself illicit, such as the narcotics trafficker.[22] Professor Ingo Walter observes that banking offshore carries dramatic costs, such as political and country risk, and increased risk of loss by embezzlement or failure of loosely regulated and uninsured banks.[23] That offshore banking havens thrive underscores the paramount value of secrecy to the haven's clientele. In addition to the advantages of maintaining anonymous accounts (or accounts held in fictitious names), banking havens frequently offer for trivial amounts of money the protective mask of anonymous and bearer corporations.[24] The bearer corporation further complicates law enforcement's mission: even if bank secrecy is pierced, law enforcement may be no nearer to discovering the beneficial owner of the funds.

Offshore banking havens have thrived partially in response to U.S. regulatory requirements and a lack of bank secrecy in the United States. A further escalation in scrutiny by law enforcement or banking regulators may have the effect of increasing the tendency to place assets abroad in secrecy jurisdictions, eroding profit centers for U.S. banks and ironically increasing the difficulty of conducting criminal investigations.[25] A wire transfer monitoring system could further heighten the competitive disadvantage of U.S. banks vis-à-vis banks in loosely regulated bank secrecy jurisdictions. This competitive disadvantage would be exacerbated by the imposition of further compliance costs on banks and by creating too large a gap between the United States and the rest of the world in terms of policing money laundering.[26]

Offshore banking havens raise a related question: would monitoring deter foreign nationals and corporations from routing their wire transfers through New York? Concerns about undermining

---

[20] *Washington Post*, March 6, 1995, p. A13.

[21] The islands are also the sixth largest source of bank loans to the United States from abroad. *Recent Developments in Transnational Crime Affecting U.S. Law Enforcement and Foreign Policy,* Hearing before the Subcommittee on Terrorism, Narcotics and International Relations of the Committee on Foreign Relations, United States Senate. S. Hrg 103-606, p. 136. Senator Kerry stated that the Cayman Islands hold some $400 billion in assets, with a population of only 26,000. *Ibid.*, p. 4.

[22] Even well-known banking havens, such as Panama under Noriega, have had legal mechanisms for piercing secrecy, such as Law 23 of December 31, 1986, permitting Panamanian officials to provide information when requested by foreign authorities. Statement of Assistant Attorney General Jo Ann Harris, S. Hrg. 103-606, p. 38.

[23] Ingo Walter, *The Secret Money Market: Inside the Dark World of Tax Evasion, Financial Fraud, Insider Trading, Money Laundering, and Capital Flight* (New York, NY: Harper & Row, 1990), p. 7.

[24] A fully anonymous shell corporation may be bought in Turks and Caicos Islands for as little as $10,000, a trivial sum in relation to the sums of money that may be laundered through it. A bearer corporation is owned by whoever holds the corporation's shares (i.e., the shares are not listed to a particular owner). Furthermore, no public records are kept as to the holder of the shares, and transfer of the corporation (and its assets) may be effected informally, by the handing off of the paper documents. Jack Blum, CSIS Conference on Global Organized Crime, September 26, 1994. Blum also noted that the relatively insignificant costs of buying anonymity would defeat any attempts to detect patterns of wires involving certain entities, so long as the launderer were willing to discard anonymous corporations after several uses.

[25] Recent U.S. efforts to control transfer pricing abuse and offshore trusts may strengthen the incentive of some to find alternative mechanisms for moving money, so as to avoid U.S. regulation and intrusions into secret movements of money.

[26] Extreme solutions to the problem posed by offshore banking havens have been proposed: in fact, the Kerry Amendment, section 4702 of the Anti-Drug Abuse Act of 1988, requires the President to bar from U.S. dollar clearing or wire transfer systems known money launderers, as well as countries and banks facilitating money laundering. 31 U.S.C. 5311, note. This provision has never been invoked.

the preeminence of the U.S. dollar as the medium for international transactions may be exaggerated, however. The financial solidity and history of gross netting of real-time payments in New York militate against mass defections to other wire transfer systems worldwide. CHIPS is the premier international payment system, and CHIPS's appeal is, and would remain, the extensive correspondent relationships of its member banks, who may then offer lower cost book transfers to complete wire transfers.

But some commentators emphasize that only historical accident has led to many international transactions relying upon the dollar as the conversion currency between two foreign currencies.[27] It is possible that, on the margins, transferors particularly valuing confidentiality might take a chance on new gross settlement wire transfer systems, particularly the one proposed by the Bank of Japan, which would also have the advantage of involvement of a central bank, a stable currency, and a stable political climate. Over time, confidence in new systems could be gained and true competition might ensue, to the detriment of U.S. payment systems with compromised confidentiality.

European and Other Data Protection Initiatives

An additional impediment to the proposed monitoring derives from European data protection initiatives governing the uses of electronically stored data and its transborder flow. These initiatives all aim to protect data generated within a country's borders, even as the data crosses international borders. Generally, information may be prohibited from leaving a signatory country if it means entering a country with less stringent data protection laws.[28] Several international bodies have already addressed the issue of electronic data protection (U.S. experts usually term this "information privacy"), with the OECD Guidelines and the Council of Europe's Convention issued more than a decade ago. For instance, on July 25, 1995, the Council of Ministers of the European Union adopted the Directive on Protection of Personal Data (the EU Data Protection Directive).[29] All of these data protection initiatives must be implemented into national law through the regular legislative channels of a signatory country before they have binding effect.

---

[27] See, e.g., Hughes, "Policing Money Laundering Through Funds Transfers," *op. cit.*, footnote 14, pp. 312-313 (citations omitted). Hughes argues that offshore netting is a distinct possibility due to enhanced recordkeeping (*not* reporting) requirements proposed by Treasury in 1990.

[28] Professor Joel Reidenberg notes several instances where, pursuant to domestic law, foreign governments have "prohibited the transmission of personal information to countries perceived as ignoring computer privacy concerns," including the French and British governments prohibiting data transfers to the United States. Joel Reidenberg, "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" 44 *Federal Communications Law Journal* 195-243, 199 & n. 16 (March 1992). David H. Flaherty, the Data Protection Registrar for the Canadian province of British Columbia, cautions that European data protectors "anticipate blocking the movement of personal data from European branches of multinationals to Canadian or American branches, because equivalent data protection does not exist." *Telecommunications Privacy: A Report to the Canadian Radio-Television and Telecommunications Commission*, 73 (1992). Currently, the Electronic Communications Privacy Act (ECPA) would sufficiently protect wire transfer data to satisfy the European and OECD initiatives. OTA is aware of no instances where international wire transfers to the United States have been barred by foreign data protection standards or commissioners.

[29] Citations to the Directive are to the "Common Position" approved February 20, 1995. Some view protection of transborder flows of information to be subtle non-tariff barriers to trade. See, e.g., the Business Roundtable Statement on Transborder Data Flow: "International Information Flow: A Plan for Action," *reprinted in* L. Richard Fischer, *The Law of Financial Privacy: A Compliance Guide* (2nd edition)(Warren, Gorham & Lamont: Boston, 1991) 6-89 to 6-125, A6.3. Others regard the EU Data Protection Directive as a "threat [to] U.S. leadership in the information economy" by its restrictions on transborder flows to the United States. Fred H. Cate, "The EU Data Protection Directive, Information Privacy and the Public Interest," forthcoming in 80 *Iowa L. Rev.*, (April 1995).

While similar in topic and scope of protection, there are substantial differences in legal effects of the various data protection initiatives and national data protection laws. At least 15 states have enacted data protection laws, including Australia, Austria, Belgium, Denmark, France, Germany, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. Others are on the brink of doing so: Finland, Iceland, and Italy.[30] While national law is ultimately what shapes data protection policies, for purposes of economy, this chapter will focus on the initiatives themselves.

In 1980, the OECD[31] issued its *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Guidelines").[32] The OECD Guidelines seek voluntary compliance by signatory states.[33] They recommend limits on the collection of data, a relevancy requirement, a 'purpose' limitation on the use of data, reasonable security safeguards, and prohibitions on disclosure without the subject's consent or authorization. Part 3 of the OECD Guidelines provides that a member country should permit the export of data to another member country, provided that the receiving country observes the guidelines' principles.

The *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* ("European Convention")[34] was concluded within the framework of the Council of Europe.[35] The European Convention is an international treaty and requires signatory states to incorporate its principles into their domestic law by normal parliamentary procedures. Until this is done, the treaty grants no rights directly to individuals within a signatory state. This "executory" status of the European Convention, as well as the EU Data Protection Directive, is significant for it underscores that national law is paramount and thus individual signatory states may treat U.S. practices regarding international wire transfers differently.[36]

Also under the aegis of the Council of Europe, the Council of Ministers has set forth sectoral recommendations for the access and dissemination of specific types of data. These solely advisory recommendations are addressed to the governments of the member states, "inviting them to take account of the solutions offered in the recommen-

---

[30] Fischer, *ibid.*, 6-9 to 6-10, ¶6.04.

[31] The Organization for Economic Corporation and Development (OECD) consists of the states of Western Europe, North America, New Zealand, and Japan. The OECD guidelines have been adopted in one form or another by 24 countries (e.g., the United States, Australia, Canada and New Zealand do not protect data handled by private corporations). Nations adopting the guidelines consist of Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. A. Neisingh, A. and J. de Houver, translated as *Transborder Data Flows* (New York, NY: KPMG, 1988), p. 27.

[32] O.E.C.D. Doc. No. C(80)58 (Final) (September 23, 1980), *reprinted in* 20 *I.L.M.* 422-427 (March 1981).

[33] Reidenberg, "Privacy in the Information Economy," op. cit., footnote 28, n. 21.

[34] Euro. T.S. No. 108 (Jan. 28, 1981) ("European Convention"), *reprinted in* 20 *I.L.M.* 317-325 (March 1981). This convention entered into force by late 1987 and until recently was the only binding international instrument on data protection.

[35] The Council of Europe consists of Andorra, Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, San Marino, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. The Convention has entered into force in Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Luxembourg, the Netherlands, Norway, Portugal, Slovenia, Spain, Sweden, and the United Kingdom.

[36] Actually, Title VI of the French Constitution, in certain circumstances, may incorporate automatically international treaties, including EU Directives, directly into French national law.

dations when they are dealing with the particular data protection issues discussed in the recommendations."[37] These recommendations include *Protection of Personal Data Used for Payment and Other Related Operations* ("the Council of Europe's Recommendation")[38].

The European Union's *Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data and on the Free Movement of Such Data* has only recently been formally adopted.[39] It is expected that it will include a provision requiring the member country's data protection commissioner to prohibit exports of "personal data" when the receiving country does not possess adequate data protection laws.[40]

The EU Data Protection Directive applies only to "personal data," defined as any information relating to an identified or identifiable *natural* person.[41] Generally, personal data may be processed only with the consent of the data subject. The data subject usually must be provided with certain mandatory disclosures if data is to be collected, processed and/or distributed to a third party. He or she must also have access to the data; the opportunity to object to its collection, processing and/or disclosure; and the opportunity to correct any factual errors.

Unresolved Questions From the Data Protection Initiatives

An initial problem in exploring the implications of these data protection initiatives stems from the term "personal data." The European Convention defines "personal data" to include any information relating to an identified or identifiable person (the "data subject").[42] National legislation implementing the European Convention generally has not extended the term "personal data" to include corporate data.[43] The Council of Europe's Recommendation notes this phenomenon, advising further that countries are free not to protect legal persons, although the Recommendation expresses solicitude for the closely held corporation, insofar as its records begin to reflect personal information.[44]

A second unresolved question is the scope of the Recommendation, the most detailed instrument regarding financial data protection. Its drafters frequently note that they intend to give the term "means of payment" as broad a reading as possible. The Explanatory Memorandum to the Recommendation underscores that the recommendation addresses at least consumer electronic payment systems, such as smartcards and electronic funds-transfer/point-of-sale transactions

---

[37] Explanatory Memorandum to Recommendation No. R(90)19, paragraph 2 (Council of Europe, 1992).

[38] Recommendation No. R (90)19 (Council of Europe, 1992).

[39] Originally issued at 1990 O.J. (C277), Com(90)314 Final SYNS 287 (Sept. 13, 1990). The Common Position of the Council of Ministers is found at 1995 OJ (C 93) (13 April 1995). Citations to the EU Data Protection are to the Common Position.

[40] Article 25(1) specifies that "Member States shall provide that the transfer to a third country of personal data. . . may take place only if. . . the third country in question ensures an adequate level of protection." American corporations "fear that they will be unable to move. . . data legally—even if they own it—to the United States." Fred H. Cate, "Protecting Information Privacy," *The Annenberg Washington Program Update,* vol. 2 no. 2 (November 1994), p. 4.

[41] Article 2(a).

[42] Article 2 subdivision a.

[43] Norway, Austria, Denmark and Luxembourg protect the records of corporations and legal persons. Fischer, 6-9, ¶ 6.04, fns. 56-58. By way of contrast, the UK Data Protection Act 1984 protects only identifiable, living persons.

[44] Op. cit., footnote 38, ¶ 31.

(EFT-POS). The references and examples of "means of payment" are consistently consumer systems: EFT-POS, automated teller machines (ATM), credit card, and, prospectively, smart card and digital money.[45] This suggests that wholesale wire transfers do not fall within the ambit of the Recommendation. The strongest evidence that the Recommendation would apply to wholesale wire transfer systems comes in an aside in paragraph 36 of the appendix: SWIFT is referenced, in excluding from the Recommendation's scope the telecommunication operator which leases a line to the "communication network operator," or SWIFT. Implicitly, it would appear that SWIFT's messages, including instructions to execute book transfers, are within the scope of the Recommendation. Nevertheless, the Recommendation is solely hortatory, and it remains to be seen whether individual states choose to bring wholesale wire transfers under their data protection regimes.

A third issue looms in the question of extraterritoriality. Could a European country draft legislation that would punish an action of a U.S.-domiciled bank or wire transfer system? Or might a signatory state hold its own banks vicariously liable for monitoring taking place in the United States? This question would arise where the European bank *must* disclose the data in order to execute the customer's wire transfer instructions. Countries with data protection laws may punish banks, both criminally and civilly, for actions of unrelated parties in foreign states.[46] The Recommendation itself sanctions the use of data in order to complete a transaction, raising the possibility that the disclosure of wire transfer data to a U.S. recipient bank would comply with the dictates of say, the German law, which holds that "personal data may be disclosed to third parties only if the disclosure serves the purpose of a contractual or [other] obligation."[47] This argument, that the disclosure is implicitly permitted, is partially undercut by the fact that the originator need not be identified by the originating bank for the transaction to be executed, hence the originator's consent

[45] For example, paragraphs 4 and 5 of The Explanatory Memorandum to the Recommendation underscore that the document addresses consumer electronic payment systems, such as smartcards and electronic- wire-transfer/point-of-sale (EFT-POS) transactions.

[46] Joel Reidenberg suggests in an upcoming article in the Iowa Law Review that countries may hold their banks strictly liable for secondary use processing in other countries, or countries may simply block the export of data if secondary use systems are in place. forthcoming in 80 *Iowa L. Rev.*, (April 1995). One example is the recent Quebec data protection law, chapter 17, *Loi sur la protection des renseignements personnels dans le secteur privé*, (adopted June 15, 1993). Any of the technological configurations set forth in chapter 7 would raise this secondary use issue, whether a U.S. bank or U.S. law enforcement was conducting the secondary use. Some U.S. banks already scan all wire transfers in seeking to comply with Office of Foreign Assets Control (OFAC) prohibitions on financial transactions with certain blocked countries and designated banks and individuals. (See discussion of the OFAC system in chapter 4).

Also, the U.K. Data Protection Act 1984 requires that data collectors register with the British government and specify potential countries that might receive data. The Act sets out civil and, potentially, criminal sanctions for violations. See World Wide Web site: http://www.open.gov.uk/dpr/dprhome.htm (May 9, 1995).

[47] The EU Data Protection Directive also speaks to the issue of transborder flow of "personal data" and may prohibit it even where the export and potential disclosure is essential to the customer's intent. One expert opines that express customer consent may not suffice to waive the proscription against the export of data to a country with inadequate data protection standards. Telephone interview, Professor Fred H. Cate, Indiana University Law School, March 14, 1995. At the same time, similar to the Recommendation, the EU Data Protection Directive's Article 26 provides exceptions to this general injunction. One exception concerns instances where the data subject has given *unambiguous* consent to the proposed transfer of data to a state which does not ensure adequate levels of protection. Article 26 further provides an exception permitting transfers of data where the transfer is necessary for performance under a contract between the data subject and the controller of the data. While the scope of Article 26 is still unclear and untested, the two exceptions noted may suffice to permit wire transfers to the United States, even if the United States monitors wire transfer traffic for money laundering.

to disclose personal data cannot be assumed from the intent to transfer funds.[48]

A final question involves the breadth of the exemption of Principle 5 of the Recommendation, which provides:

> Personal data collected and stored for the purposes referred to in principles 3.1 and 4.1 [so as to provide service, verify legitimacy of transactions, and manage accounts] may only be communicated in the following cases:
>
> a. in accordance with obligations laid down by domestic law;
>
> b. when it is necessary to protect the essential and legitimate interests of the body providing the means of payment;
>
> c. with the express and informed consent of the individual. . . .

Paragraph 62 of the Explanatory Memorandum notes that "obligations laid down by domestic law" extend beyond statutory duties to communicate data and court orders to cases where:

> . . . it is in the public interest to reveal personal data for the purpose of crime *prevention*. It may be the case that a body providing a means of payment strongly suspects that illegally acquired funds are being laundered through it by an account holder. Such circumstances would justify the communications of the relevant data to the police.[49] [emphasis added]

An aggressive reading of the first clause of paragraph 62 might argue that prevention of money laundering would require communicating wire transfer records to the authorities to detect money laundering, although this reading is clearly undercut by the second and third sentences, which refer to account-specific suspicion. Hence, this suggests a bootstrap problem in the case of wire transfers: the only justification for secondary processing and disclosure of personal data would be "crime prevention" but as the bank (particularly the intermediary bank) likely will be unaware of criminal conduct in advance, such potential criminal conduct will likely go undiscovered in the flood of wire transfers passing through the bank's wire room. Subsection 5.1.b suggests another interesting argument, that in order to protect the "essential and legitimate interests" of payment systems in their integrity and freedom from money laundering, disclosure might be permitted, although these arguments are scarcely certain enough to encourage foreign originating banks to risk violating data protection laws.[50]

INTERNATIONAL LAW ENFORCEMENT EFFORTS

Unilateral Efforts of the United States

U.S. law enforcement efforts to curtail money laundering have not stopped at the border. Al-

---

[48] This would not be true if the United States barred U.S. recipient banks from handling transfers with unidentified originators; however, the U.S. Treasury Department proposed this in its 1989 advance notice of rulemaking only to withdraw it after adverse banking industry comments. See 54 *Fed. Reg*. 45769 (Oct. 31, 1989), and 55 *Fed. Reg*. 41696 (Oct. 15, 1990).

[49] Article 13 of the EU Data Protection Directive contains a similar clause permitting member states to adopt legislative measures restricting the Directive's scope with respect to a broad class of law enforcement activities, including "the prevention, investigation, detection and prosecution of criminal offences." This clause emphasizes the difficult relationship between principles of fair information practices and the mission of law enforcement in the information age. This exemption covers Article 6(1), which sets forth principles for processing of data, but the exemption does not sanction departures from the article governing the transfer of data to third countries. Earlier, "processing" is defined broadly, to include dissemination and disclosure. The upshot is that the precise treatment of law enforcement and secondary use of data is rather unclear, and may only be settled in individual national implementation of the EU Directive.

[50] A parallel question arises in the context of the EU Data Protection Directive's Articles 3(2) and 13(d), which provide that the Directive shall not apply to the processing of personal data concerning the activities of the State in areas of criminal law; and that member states may restrict the scope of some of the Directives articles when necessary to safeguard law enforcement's mission. These provisions are by no means an unambiguous grant of an exception to law enforcement: for example, it is not clear whether Article 3(2) permits private sector disclosure of data as well as law enforcement processing. All of the initiatives seek to limit disclosure of data and it is this disclosure which is integral to any monitoring proposal.

though U.S. efforts might appear to some to be extraterritorial overreaching and a threat to the sovereignty of other states,[51] a state may properly assert jurisdiction beyond its borders in certain circumstances. One longstanding rule of international law permits a state to assert jurisdiction over its nationals no matter where they might be, if they commit a criminal act.[52] Moreover, states may assert jurisdiction even over non-nationals not present within their borders when the individual commits a crime whose effects are felt in that state. A well-known example of this is the U.S. prosecution of Manuel Noriega in South Florida for his money laundering and narcotics trafficking operations based in Panama.[53] Many foreign governments, including close allies of the United States, take issue with these extraterritorial bases of jurisdiction, out of a belief that jurisdiction ends with the territorial boundaries.[54]

The Restatement's principles are echoed in the U.S. money laundering statute, asserting jurisdiction over money laundering where

> (1) the conduct is by a United States citizen, or in the case of a non-United States citizen, the conduct occurs in part in the United States; and (2) the transactions or series of related transactions. . . . exceeding $10,000.

The United States' assertion of jurisdiction passes the muster of international legal principles as understood by U.S. courts, subject to the requirement of "reasonableness."[55] Prior to prosecution, however, targets must be identified. Unilateral efforts of the United States to investi-

---

[51] Jack Blum, S. Hrg. 103-606, p. 133. An authority on Caymanian commercial and banking law has opined that "[n]o area in international legal affairs has . . . caused more tension between governments than [the extraterritorial] investigative power of United States grand juries." Ian Paget-Brown, "Bank Secrecy and Criminal Matters: Cayman Islands and U.S. Cooperative Development," 20 *Case Wes. J. Int'l L.* 369-391, p. 379 (March 1988).

[52] The French adhere to this principle, for example. *See also* Paget-Brown, who notes that the United States may exercise jurisdiction over its citizens both within and without the United States, as well as "over all persons who purposefully avail themselves of the privilege of conducting activities within the United States and thereby invoke the benefits and protection of its laws." *Ibid*., p. 378

[53] The eminent American Law Institute publishes the Restatement of the Law series, an influential reformulation of legal rules drawn from judicial opinions and other sources. Section 402 of the Restatement of the Law (3d) the Foreign Relations Law of the United States specifies that a state has jurisdiction to prescribe law with respect to:

(1) (a) conduct that , wholly or in substantial part takes place within its territory;

(b) the status of persons, or interests in things present within its territory;

(c) conduct outside its territory that has or is intended to have substantial effect within its territory;

(2) the activities, interests, status or relations of its nationals outside as well as within its territory; and

(3) certain conduct outside it territory by persons not its national that is directed against the security of the state or against a limited class of other state interests.

Subsection (3) is often referred to as the "protective principle," for such matters as conspiracies to violate immigration/customs laws, counterfeiting and arguably money laundering, with its potential for destabilization—some sources indicate that as much as 60 percent of US funds are held abroad. The Polish Penal Code of 1969 parallels these jurisdictional bases, providing that the criminal code may be applied to offenses committed by Polish citizens wherever they might be (Article 113), as well as to offenses of non-Poles outside of the territorial boundaries of Poland, as long as the conduct either violates the laws of the other country or runs counter to the political or economic interests of Poland (Articles 114 and 115).

[54] The U.N. *Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* provides support for this view in article 2(3): a signatory state is expected to defer to the territorial boundaries of other states and not attempt to exercise jurisdiction for acts occurring there, as long as that state exclusively reserves jurisdiction. At least one commentator on multilateral cooperative efforts cautions against U.S. unilateral actions and *realpolitik* for fear that they undermine the legitimacy of diplomacy, urging instead additional U.S. efforts aimed at building new and strengthening existing international organizations and treaties to combat money laundering. Bruce Zagaris, "Developments in International Judicial Assistance and Related Matters," 18 *Denver J. Int'l Law and Policy,* 339-386, 384-85.

[55] See Todd C. Jones, "Compulsion over Comity: The United States' Assault on Foreign Bank Secrecy," 12 *Northwestern J. of Int'l Law & Business* 454-507, 486-487, *citing* the Restatement (Third), 403(2).

gate potential international money laundering (by U.S. citizens or others) have been stymied by the laws of other states.[56] This leads to the paradoxical result that although the U.S. may properly exercise criminal jurisdiction over money launderers extraterritorially, foreign bank secrecy and data protection initiatives may bar U.S. law enforcement from identifying international money launderers. Alternative avenues have been pursued, notably bilateral and multilateral agreements (addressed below), some of which expressly address the question of foreign bank secrecy as an impediment to investigations of money laundering.

Multilateral Cooperation and Agreements

Beyond unilateral efforts at stopping international crime, the United States has both stimulated and joined international efforts to make law enforcement itself transnational, soliciting cooperation and building alliances with foreign partners. The United Nations *Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* (the Vienna Convention) was signed in Vienna on December 20, 1988 and entered into force on December 11, 1990.[57] International cooperation in pursuing money laundering has been surprisingly wide ranging and successful, if judged by the numbers of organizations created and conventions drafted. Foremost among international organizations combating money laundering is the Financial Action Task Force (FATF), created at the International Economic Summit of 1989 as a mechanism for international cooperation in fighting narcotics-related money laundering. FATF seeks to improve contact between experts and law enforcement authorities in member countries, document money laundering techniques and compile national programs targeting money laundering. FATF now has members from 26 countries.[58]

Urged on by the sense of Congress that money laundering is an international crime whose defeat cannot be achieved without involving international cooperation and agreements,[59] the United States has been instrumental in the FATF's work, especially its efforts on agreements directed at information sharing between law enforcement agencies in different countries. FATF has made 40 recommendations to its member states pertaining to money laundering. The most significant recommendations are the requirements that member states make drug money laundering a criminal offense (Recommendation 4); that member states permit banks to report suspicious transactions to the competent authorities (Recommendation 16); and that member states should not permit financial institutions to keep anonymous accounts (Recommendation 12). By the 1994 Annual Report of the FATF, all member governments permitted reporting of suspicious transactions, and 19 member governments required their banks to report such transactions. While many federal officials laud the successes of FATF in marshaling the states of the world in the battle against money laundering, at least one outside expert cautions that FATF's rhetoric outstrips its performance, pointing specifically to the slowness with which some core FATF members have implemented the forty recommendations.[60]

---

[56] See also box 6-1 in this chapter discussing the limits on the use of subpoenas to obtain records created and maintained abroad.

[57] On June 10, 1994, Colombia became the 101st signatory state to the Vienna Convention, which obligates signatory states to criminalize money laundering incident to narcotics trafficking. Article 3(b).

[58] Members of FATF include the countries of G-7 and the European Union, as well as Hong Kong, New Zealand, Australia, Singapore, Switzerland, and Turkey. Each member is entitled to representatives from its Ministries of Finance, Justice, and Foreign Affairs and its central banking system, and there are official "observers" from several international institutions.

[59] Sections 4101-4108 of the Anti-Drug Abuse Act of 1988 (Pub. L. 100-690, Title IV).

[60] Telephone interview with Bruce Zagaris, Esq., Cameron & Hornbostel, March 14, 1995.

At its most recent meeting, in 1994, the FATF explicitly broadened its mission to encompass non-drug-related money laundering. Its current goals are 1) expanding members' money laundering legislation so that money laundering prosecutions need not depend on proof of an underlying crime;[61] 2) monitoring members for implementation of the recommendations;[62] 3) monitoring developments in money laundering; and 4) encouraging the formation of regional task forces patterned after itself, such as the Caribbean Task Force and the Gulf Cooperation Council. FATF's 40 recommendations have already become the basis of rules adopted by the Caribbean Financial Task Force. The Caribbean Task Force also signed an Memorandum of Understanding with Great Britain to work on white collar crime, including money laundering, among its members.[63]

Other groups have been created in the Western Hemisphere to combat money laundering. The Organization of American States (OAS) in its 1990 meeting condemned illicit drug trafficking and money laundering and endorsed international agreements and cooperative efforts aimed at eliminating trafficking in narcotic drugs.[64] Soon thereafter, an Inter-American Commission on Drug Abuse Control (CICAD) put forth *Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Related Offenses.*[65] The CICAD proposals include provisions intended to remove bank secrecy as an impediment to access to banking records, as well as a proposal for civil sanctions in case of bank failure to keep records and report suspicious transactions.[66] The CICAD plan extends the definition of money laundering beyond the narcotics context.[67] It seeks to regulate broadly defined "financial institutions," prohibit anonymously held bank accounts, and require financial institutions to identify and verify their customers.[68] It also requires currency transaction reporting (with an express waiver of bank secrecy or confidentiality), prohibits structuring, and mandates suspicious transaction reporting, with safe harbor provisions for banks.[69]

In addition to these groups, the Commission of the European Communities, in 1991, issued a directive compatible with (and in some cases exceeding) the FATF recommendations.[70] The Council of Europe also passed a multilateral money laundering convention signed by 13

---

[61] Interview with Rayburn Hesse, Chief of International Narcotics Matters, Department of State, July 28, 1994. "Donor Members" of FATF (those whose donations finance the Caribbean Financial Action Task Force and other FATF activities) are the United States, the United Kingdom, France, the Netherlands, and Canada.

[62] Each year, four or five countries are chosen, with fellow members conducting detailed audits of those countries' compliance with the Recommendations. Reports of findings are issued.

[63] Fred Verinder, Deputy Assistant Director, Criminal Division, FBI, testimony in *Hearing Before the Committee on Banking, Finance and Urban Affairs*, House of Representatives, "Federal Government's Response to Money Laundering," 103rd Cong., 1st Sess., 103-40, May 25-26, 1994, p. 40.

[64] OAS General Secretariat, "Declaration and Program of Action at Ixtapa," Washington, DC, 1990.

[65] The Model Regulations have been twice endorsed by the 34 member states of the Organization of American States, (OAS) once at the annual OAS general assembly in May 1992, and more recently at the Summit of the Americas, in December, 1994. AG/doc.2916/92 rev.1.

[66] FATF's 40 recommendations became the basis of rules endorsed by the OAS.

[67] "Miami summit slights OAS proposals, agrees to more talk," *Money Laundering Alert*, Dec. 1994, p. 5; Charles A. Intriago, "OAS Unit Proposes Money Laundering, Forfeiture Laws," *North-South*, vol. 1, No. 2, August-September 1992, pp. 38-39.

[68] Article 9 ("financial institutions") and Article 10.

[69] Articles 12 through 14 and 19. In this context, "safe harbor" denotes a legislatively conferred immunity from criminal or civil liability for disclosures mandated by governments.

[70] Some sense of the gap between rhetoric and reality is evidenced by the fact that Ireland only in 1994 implemented the European Community (EC) directive by passing anti-money laundering legislation.

OECD members (and expected to be signed by four more).[71] The increased freedom of movement of people, goods, information, and currencies that will occur as the single market becomes a reality has increased concern over money laundering in Europe, and the concern is further stimulated by new awareness of organized crime, drug trafficking, and money laundering within the countries of Central and Eastern Europe. Some EU countries are now considering further legislation to combat money laundering.[72]

The Bank of International Settlements (BIS)[73] has a task force to build international cooperation in control of money laundering. International financial leaders, according to some observers, were at first hesitant to deal with the problem of abuse of bank secrecy laws. Some also feared that banks in countries such as Luxembourg had unknowingly become dependent on illicit money flowing through their accounts.[74]

The apparent cooperation is somewhat surprising in light of the lingering, if false, perception that money laundering is a predominantly American problem and the fact that possession of, if not trafficking in, cannabis and some opiates, is legal or tolerated in some of the United States' allies within the European Union. Additionally, independent of the legal status of narcotics themselves, some European states focus state efforts to prevent drug abuse on rehabilitation and education instead of on law enforcement. Beyond the narcotics context, there have been great differences in perspectives on tax evasion and avoidance, as well as some other kinds of white collar crime, impairing concerted action against all forms of money laundering. At the same time there are indications that Europe, at least, is awakening to the destabilizing threat that money laundering poses. Europol, the new multinational European police force, now has jurisdiction over money laundering in addition to its former jurisdiction over drug offenses.[75] Other states are also awakening to the destabilizing force of money laundering and its role in terrorism, arms sales and political unrest. U.S. private banking officers and regulators often meet with foreign officials and stress these less financial motives for money laundering, in seeking to create a stronger consensus for combating international money laundering.

Bilateral Conventions and Cooperation

The United States has invested much capital in the negotiation of bilateral accords aimed at facilitating prosecutions of crime with international dimensions. Mutual Legal Assistance Treaties (MLATs) represent a considerable improvement over the older vehicles of letters rogatory and MATs (Mutual Assistance Treaties). Nevertheless, MLATs do not suffice to permit suspicionless

---

[71] "Money Laundering Experts Team Up—On and Off the Job," *Bank Management*, March 1991. Thus far only six signatory countries have implemented its terms. This signifies some of the difficulties of international cooperation, even among the closest of allies. A further example of this would be Mexico, whose legislature has been struggling to criminalize money laundering for four years now, without reaching finality. Telephone interview with Bruce Zagaris, March 14, 1995.

[72] J. Stewart-Clark, "Security Concerns in the European Community," *Police Chief*, vol. 60, No. 10, (1993), pp. 57ff.

[73] The Bank of International Settlements (BIS) was created in 1930 to promote central bank cooperation, and founded the "Basle" Committee to address international banking supervision issues, including developing a code of conduct for bank monitoring to keep financial systems free of criminal money. See Jones, "Compulsion over Comity," *op. cit.*, footnote 54, pp. 481-82, and footnotes. The Basel Statement of Principles, agreed to on December 12, 1988, are designed to fight money laundering in the banking system by promoting measures such as customer identification, cooperation with law enforcement to extent permitted by bank secrecy or confidentiality laws, and refusal to assist suspicious transactions.

[74] Brian R. Allen, "The Banking Confidentiality Laws of Luxembourg and the Bank of Credit & Commerce International," 28 *Texas Int'l L. J.*, 73-117 (Winter 1993). Luxembourg, a major banking center, now has stiff penalties for money laundering, but only three bank examiners. Verinder, *op.cit.*, footnote 63.

[75] *Money Laundering Alert*, December 1994, p. 8.

and indiscriminate access to records held abroad,[76] and in fact, unilateral U.S. efforts targeting international wire transfers may threaten the success of the MLAT process as well as other multilateral efforts detailed above.

Under MLATs, governments take on international legal obligations to provide legal assistance to each other.[77] MLATs strengthen the procedures for international cooperation, and create binding procedures, obligations and channels of communication for exchange of information and evidence in criminal investigations and proceedings.[78] The requesting country does not need to rely solely upon judicial comity to obtain the legal assistance sought (as with letters rogatory). MLATs may extend to a broader class of crimes than MATs, although they may exclude tax evasion, particularly so in treaties executed with banking haven countries, such as the Bahamas and the Cayman Islands, whose MLATs cover relatively narrow classes of crimes. The Panamanian MLAT provides a mechanism for obtaining currency transaction information accessible to the Panamanian government.

MLATs are drafted with a view towards helping ongoing investigations, and have their best success when U.S. authorities can substantiate their suspicion regarding an individual subject to foreign jurisdiction. This form of cooperation can be unwieldy: requests percolate up from the field to the Department of Justice's Office of International Affairs, thence to the Department of State and the foreign country, where the process is repeated in reverse, although MLATs may provide for requests to be forwarded directly from law enforcement agency to law enforcement agency abroad.[79]

Recently, the United States has negotiated bilateral pacts targeting money laundering; these agreements seek improved quality of information regarding currency transactions and provide avenues for sharing that information between countries. Examples of these agreements are Financial Information Exchange Agreements (FIEAs).[80] FIEAs generally require signatory countries to "ensure that. . . financial institutions. . . record currency transaction information. . . and transfer said information to their respective executing agencies. . . . "[81] and to share those records internationally. But the signatory states promise only to "provide each other the fullest measure of mutual cooperation. . . . "[82]

---

[76] The Office of International Affairs, Criminal Division, Department of Justice, avers that MLATs envision a wide range of legal assistance, even at the early stages of an investigation. Nevertheless, most configurations of a wire transfer monitoring system aim at *detecting* a possible crime so that an investigation may be opened, at which point, the MLAT could be invoked. The MLAT executed with the Cayman Islands illustrates this point. While it provides for mutual assistance in "investigation, prosecution, and suppression of [specified] criminal offenses," a party may deny a request for assistance where "the request does not establish that there are reasonable grounds for believing that the criminal offense specified in the request has been committed. . . . " *United Kingdom-United States: Treaty Concerning the Cayman Islands and Mutual Legal Assistance in Criminal Matters* (July 3, 1986), *reprinted in* 26 *I.L.M.* 536-549, Articles 1 and 3(c)(i). Moreover, the request for assistance shall include "information concerning the persons involved including, where available, their full names, dates of birth, and addresses. . . . " Article 4(2)(b). This is precisely the sort of information that a monitoring system would be attempting to discover.

[77] The first MLAT was executed with Switzerland on May 25, 1973. 27 U.S.T. 2019, T.I.A.S. No. 8302 (entering into force Jan. 23, 1977). Other MLATs have been negotiated with some bank secrecy jurisdictions, including the Bahamas, the Cayman Islands, Canada (a blocking jurisdiction) and the Netherlands (including the Dutch-Antilles).

[78] As one commentator notes, MLATs facilitate the investigation of crimes beyond producing evidence for the trials of previously indicted defendants. Napp, "Mutual Legal Assistance Treaties," *op. cit.*, footnote 14, p. 410.

[79] Zagaris, *op cit*., footnote 54, p. 352.

[80] The Anti-Drug Abuse Act of 1988 expressly urged the executive branch to negotiate these agreements, as well as the creation of the Financial Action Task Force. The first was with Venezuela in November of 1990; and Colombia, Ecuador, Panama, Peru, Paraguay, and most recently, Mexico (Oct. 28, 1994).

[81] Drawn by way of illustration from Article II, section (1) of the FIEA executed with Colombia on February 27, 1992.

[82] Article II, section (2) of the Colombian FIEA.

The utility of FIEAs will become clear in coming years, although many of the countries signing FIEAs are just beginning to police large cash transactions. For instance. Mexico, in agreeing to its FIEA with the United States, has agreed to share information that Mexican bank regulators do not currently require be held.[83] However successful these FIEAs will be in improving currency transaction information on an international level, they cannot provide a mechanism for sharing wire transfer information in real or near real time. The FIEAs require that the requesting law enforcement agency detail the charges against the individual whose currency transaction record are sought. Clearly, this does not square with one of the aims of a wire transfer monitoring system—detection beyond the investigation of existing leads.

A possible model for international cooperation in investigating international crime is provided by the efforts of the Securities Exchange Commission (SEC), which has had some signal successes in policing a similar problem in foreign anonymous financial activity in the United States—insider trading on the New York Stock Exchange through Swiss and other bank accounts. In a series of cases from the mid-1980s, the SEC persuaded Swiss authorities to disclose the identities of its customers who had initiated massive stock purchases immediately before takeover announcements. The differences between the SEC cases and wire transfers are plain, however: for one, the point of the wire transfer monitoring proposal is to identify hitherto unknown money laundering, not as in the case of the SEC, to identify the real party in interest to trades already recognized as very suspicious. The SEC has been able to demonstrate the clear violation of U.S. insider trading law, based on dramatic shifts in stock prices in advance of disclosures of material information, before requesting foreign banks and law enforcement to pierce bank secrecy.[84] This distinction aside, an interesting commonality exists regarding the extraterritorial enforcement of U.S. laws abroad. Just as money laundering has not been uniformly criminalized throughout the world, neither has insider trading, and yet the United States has been able to pierce bank secrecy.

THE STRUGGLE OF SOVEREIGNS

At a more abstract level, this conflict between access and financial confidentiality implicates competing assertions of sovereignty: the sovereign right of the originator state to shield the data with the protections of the originating jurisdiction and the right of the United States, or recipient state, to enforce its laws and protect its borders.[85] This conflict resembles previous U.S. attempts to enforce its antitrust laws and gain access to information held internationally by multinational corporations, an effort which gave rise to blocking statutes in the first place, but with the significant difference that the wire transfer is both a transborder flow of data and an act in itself, the import or export of money. Nonetheless, as global networks bring the world closer together, they also run the risk of exacerbating conflicts between sovereignty, conflicts which prior modes of communication and finance left latent.

As noted above, the United States has always maintained its right to prosecute individuals for criminal actions committed abroad that have impacts within the territorial confines of the United States. In addition, with the successful efforts of

---

[83] Previous to signing the FIEA, Mexican authorities merely issued nonmandatory guidelines encouraging bank recordkeeping of cash transactions. Telephone interview with Joseph Myers, Asst. Legal Counsel, FinCEN, May 28, 1995.

[84] In structure, this is no different from the need to show a magistrate probable cause of criminal conduct before a search warrant is issued for a search of U.S. account records may be searched under the legislative requirements of the U.S. Right to Financial Privacy Act.

[85] When the Supreme Court looked at the foreign bank account reporting requirements of the Bank Secrecy Act (BSA) in *California Bankers Ass'n.* v. *Shultz*, the Court emphasized the plenary powers of Congress in regulating foreign commerce and expressly drew the analogy between the holding of foreign bank accounts by U.S. citizens and the crossing of international boundaries, with the implication that the sovereign has an near absolute right of inspection. 416 U.S. 21, 62-63 (1974).

FATF in criminalizing money laundering in other countries, the extradition of money launderers is increasingly possible, as the prerequisite of the alleged offense being a crime in both countries can now be satisfied. The enforcement gap remains, however, in the problem of detecting the money laundering as wire transfers pass through the United States.[86]

CONCLUSION

Foreign bank secrecy and data protection laws present considerable barriers to the success of any monitoring system requiring indiscriminate access to wire transfer records. Moreover, U.S. efforts to unilaterally forge ahead and scrutinize wire transfer records could undermine what successes international cooperative efforts have borne, so far, such as considerable use of the MLAT procedure for aiding investigation and prosecution of money launderers and narcotics traffickers, among others. U.S. monitoring efforts also could undermine the attractiveness of the U.S. dollar as a means of international payments and disadvantage U.S. banks in the competitive marketplace of international financial services.

Should Congress decide in favor of a monitoring system, it will be essential to negotiate with the European Union and seek to obtain a policy statement that the EU Data Protection Directive is not meant to limit the ability of countries to scrutinize payment system information for money laundering.

[86] This is not to suggest that the United States is fully open to the inquiries of foreign law enforcement. In fact, ratification of MLATs has been held up in the Senate precisely out of a concern that they would permit fishing expeditions by foreign law enforcement agencies, contrary to the dictates of the Fourth Amendment. *See* Zagaris, *op. cit.*, footnote 54, p. 356. Moreover, when FinCEN negotiates international information sharing agreements, it requires that the request for BSA data be justified.