9-1-2000

Internet Casinos: A Sure Bet for Money Laundering

Jon Mills

Follow this and additional works at: <http://elibrary.law.psu.edu/psilr>

Recommended Citation

Mills, Jon (2000) "Internet Casinos: A Sure Bet for Money Laundering," *Penn State International Law Review*: Vol. 19: No. 1, Article 4.
Available at: <http://elibrary.law.psu.edu/psilr/vol19/iss1/4>

This Article is brought to you for free and open access by Penn State Law eLibrary. It has been accepted for inclusion in Penn State International Law Review by an authorized administrator of Penn State Law eLibrary. For more information, please contact ram6023@psu.edu.

Internet Casinos: A Sure Bet for Money Laundering

Jon Mills*

Since the end of World War II, American society has seen the emergence of technology promising to make life easier, better and longer lasting. The more recent explosion of the Internet is fulfilling the dreams of the high-tech pundits as it provides global real-time communication links and makes the world's knowledge universally available. Privacy concerns surrounding the development of the Internet have mounted, and in response, service providers and web site operators have enabled web users to conduct transactions in nearly complete anonymity. While anonymity respects individual privacy, anonymity also facilitates criminal activities needing secrecy. One such activity is money laundering, which is now being facilitated by the emerging Internet casinos industry. These casinos can be physically located anywhere with web sites available worldwide. Internet casinos were a target of legislation by the United States Congress, but the legislation, the Internet Gambling Prohibition Act, failed to pass. So, at the moment, Internet casinos are a virtually unregulated mechanism for laundering illegal funds.

This problem crosses national boundaries. Consequently, the nations concerned with preventing money laundering must cooperate. The United States has enacted a host of laws that enable the government to prosecute both the root crime of money laundering, as well as the means, on-line gambling. But, effective eradication of this criminal enterprise will require international cooperation.

* Interim Dean, Professor of Law & Director of Center for Governmental Responsibility, University of Florida, Levin College of Law.

A. *Money Laundering and Internet Casino Industry*

The greatest criminal threat posed by the blossoming virtual gaming industry is the unprecedented potential it presents for criminal elements seeking to launder their ill-gotten gains.¹ Current estimates suggest that between \$300 and 500 billion dollars are laundered each year,² and many prosecutors agree that it is easy and economical to launder criminal proceeds through offshore casinos.³ For example, when Florida plays Florida State in football, place a bet on each team. Regardless of the outcome, and provided the gambler has properly structured the bets, the gambler will lose the bet placed on the losing team, but the bet on the winning team will be paid double; all the gambler has really lost is the "vigorous," the house or bookie's cut. In a similar fashion, offshore, and hence, invisible, profits can be created, or visible, and hence, declarable and deductible, losses can be generated. Dirty money has been laundered.⁴

More broadly, money laundering is the process of "placing the illegally-acquired money into the global financial system without raising suspicion: depositing it into a bank, conducting a number of transactions with the money to create a confusing or hidden audit trail, and then withdrawing the funds."⁵ Following the passage of the Money Laundering Control Act of 1986,⁶ criminal proceeds are "perpetually illegal" and criminals must, therefore, launder their illegal profits in order to facilitate their use.⁷ If the funds from a criminal enterprise are not laundered before they are spent, the spender is more likely to face tax evasion charges, prosecution

1. See *New Technologies Contain Potential for Massive Fraud*, BANKING POL'Y REP., Mar. 4-18, 1996, at 36 [hereinafter *New Technologies*].

2. See Lisa A. Barbot, Comment, *Money Laundering: An International Challenge*, 3 TUL. J. INT'L & COMP. L. 161, 163 (1995); Scott Sultzer, Comment, *Money Laundering: The Scope of the Problem and Attempts to Combat It*, 63 TENN. L. REV. 143, 146 (1995). See also Konstantin D. Magliveras, *Defeating the Money Launderer – The International and European Framework*, 1992 J. BUS. L. 161 (1992).

3. See Steven Crist, *All Bets are Off*, SPORTS ILLUSTRATED, Jan. 26, 1998, at 90.

4. See John E. Hogan, Comment, *World Wide Wager: The Feasibility of Internet Gambling Regulation*, 8 SETON HALL CONST. L.J. 815, 823 (Summer 1998).

5. Rajeev Saxena, Note and Comment, *Cyberlaundering: The Next Step for Money Launderers?*, 10 ST. THOMAS L. REV. 685, 691 (1998).

6. 18 U.S.C. §§ 1956, 1957 (1994).

7. See 18 U.S.C. § 1956 (1994); see also *United States v. Jensen*, 69 F.3d 906, 912 (8th Cir. 1995).

relating to the original criminal activity and the loss of the funds altogether.⁸

It is therefore important to realize that the laundering of money does not make that money legal. Again, it remains perpetually illegal. The effort to launder money is made to render detection of the illegal activities, and their profits, difficult, if not impossible.

Laundered criminal funds are both an end in themselves, as the "reward" for criminal endeavors, and also a means of funding further criminal acts, including, but certainly not limited to "funding terrorism and organized crime, hiding taxable income, and generally making a variety of crimes, which range from smuggling to counterfeiting, appear to be legitimate enterprises which are highly profitable."⁹ However, in the past, laundering funds was more difficult because of the built-in mechanisms and the necessity of funneling the funds through traditional, and highly regulated, financial institutions. Emerging technology, including the Internet's cyber-banking industry, will "revolutionize" the money laundering process and make it significantly easier for launders to insert dirty money into the stream of international commerce, to churn, or wash it, through legitimate businesses and hide its origin, and then to withdraw the money, ready to be spent.¹⁰ The nature of the Internet allows transactions to occur almost instantaneously and with anonymity, thus allowing the criminal launderer to avoid detection because there is no trail to follow, and, since no traditional financial institutions have been involved, there are no red flags alerting the law enforcement to the possibility of criminal activity.¹¹

B. Money Laundering Is Illegal and Statutorily Prohibited

"The United States is certainly one of the leading money laundering nations in the world,"¹² and there are innumerable ways money can be laundered. It can be smuggled out of the United States, laundered in another country that has relaxed banking

8. See Emily J. Lawrence, Note, *Let the Seller Beware: Money Laundering, Merchants and 18 U.S.C. 1956, 1957*, 33 B.C. L. REV. 841, 841 (1992).

9. Saxena, *supra* note 5, at 687.

10. See New Technologies, *supra* note 1, at 36.

11. See Bruce Zagaris & Scott B. MacDonald, *Money Laundering, Financial Fraud, and Technology: The Perils of an Instantaneous Economy*, 26 GEO. WASH. J. INT'L & ECON. 61, 63 (1992).

12. Fletcher N. Baldwin, *Money Laundering and Wire Transfers: When the New Regulations Take Effect, Will they Help?*, 14 DICK. J. INT'L L. 413, 415 (1996).

regulations or strict secrecy laws, and then returned the States once it has been adequately layered, or mixed, with legitimate funds.¹³ Or, a money launderer can acquire a legitimate business, preferably one with a large volume of cash transactions, and show the illegal proceeds as profit generated by the presumptively legal, and profitable, business.¹⁴ Alternatively, a money launderer can deposit the illegal funds in a bank, and by transferring sums less than \$10,000, create a "legitimate" history of the funds. However, due to the reporting requirements, "structuring" is not practical for large-scale money laundering operations.¹⁵

Using one of the three primary wire systems, a money launderer can, via instructions sent from one bank to another, have funds transferred from one account to any other account(s). It is easy to hide illegal funds among the millions of transfers affected by these systems, which transferred \$474 trillion among various banks in 1995 alone.¹⁶ A money launderer could launder his illegal funds by expatriating them, and then using them as collateral for a loan in the foreign jurisdiction. He would now repatriate the loaned funds as legally acquired. If the money launderer selected a foreign nation with strict banking secrecy laws, any law enforcement authority would be able to trace the loaned funds only as far back as the originating bank, but not to the client who received the loan from the bank.¹⁷ Foreign banks are also used for their "payable through" accounts, which they maintain at banks in the United States. The foreign bank will transfer all funds between it and the

13. See Sultzer, *supra* note 2, at 150, 186-187 (The United States Postal Service is often chosen for its reliability in removing and reintroducing illegal funds into the United States economy). See also John J. Fialka, *Drug Dealers Export Billions of Dollars to Evade Laws on Currency Reporting*, WALL ST. J., Apr. 7, 1994, at A4.

14. See Sultzer, *supra* note 2, at 156 (Businesses suited to money laundering activities include restaurants, bars, clubs, adult entertainment establishments, gas stations, video rental stores and parking garages).

15. See *id.* at 152. See also Frank C. Razzano, *American Money Laundering Statutes: The Case for a Worldwide System of Banking Compliance Programs*, 3 J. INT'L L. & PRAC. 277, 280-281 (1994); Sarah N. Welling, *Smurfs, Money Laundering, and the Federal Criminal Law: The Crime of Structuring Transactions*, 41 FLA. L. REV. 287, 288 (1989); Gerard Wyrsh, Comment, *Treasury Regulation of International Wire Transfer and Money Laundering: A case for a Permanent Moratorium*, 20 DENV. J. INT'L L. & POL'Y, 515, 515 n.1 (1992).

16. See Wyrsh, *supra* note 15, at 515, 518-520 (The three primary wire systems are the Federal Reserve Communications System (Fedwire), the Clearing House Interbank Payments System (CHIPS), and the Society for Worldwide Interbank Financial Telecommunications S.C. (SWIFT)). See also Sarah J. Hughes, *Policing Money Laundering Through Fund Transfers: A Critique of Regulation Under the Bank Secrecy Act*, 67 IND. L. J. 283, 290-291.

17. See Saxena, *supra* note 5, at 695.

U.S. bank through that account, and often give customers permission to conduct their own banking business out of the same account. These accounts are usually not as closely monitored because the foreign bank is expected to transfer large amounts through such an account.¹⁸

The Financial Action Task Force (FATF)¹⁹ was created in an effort to coordinate and augment international anti-money laundering efforts.²⁰ This Task Force works with other international organizations, including the International Criminal Police Organization (Interpol) and the Inter-American Drug Abuse Control Commission (CICAD) of the Organization of American States.²¹ In the United States, the parallel organization is the FinCEN, an offshoot of the Treasury Department, that "evaluates money laundering threats, supports law enforcement agencies and implements the Bank Secrecy Act."²² It is designed to "serve as a central source for financial analysis and intelligence retrieval to assist in money laundering and other financial crimes investigations."²³ Significantly, FinCEN collects data from the CTRs and SARs which financial entities file.²⁴

Beginning in the 1970s, Congress enacted several acts designed to deter money laundering and tax evasion. The Bank Secrecy Act, a part of the Bank Records and Foreign Transactions Act, was prompted by concerns that foreign banks were being used to launder funds, a crime itself, as well as to evade applicable U.S. taxes.²⁵ The Bank Secrecy Act requires transactions over \$10,000 to

18. See *Money Laundering Trends*, MONEY LAUNDERING L. REP., Feb. 1997, 1, 7.

19. Created in 1989 at the G-7 Paris Summit. See Barbot, *supra* note 2, at 173.

20. See *id.* at 173.

21. See Barbot, *supra* note 2, at 175-177 (citing Bruce Zagaris & Shiela M. Castilla, *Construction of International Financial Enforcement Subregime: The Implementation of Anti-Money Laundering Policy*, 19 BROOK. J. INT'L L. 871, 884 (1993)). See also Hans-Albrecht Schraepfer, *DIRECTORY OF INTERNATIONAL ORGANIZATIONS* 158 (1996).

22. *Efforts to Fight Financial Crimes: Hearings Before the Subcomm. on General Oversight and Investigations of the House Comm. on Banking and Financial Serv.*, 105th Cong. (1997) (statement of Rep. Spencer Bachus (Rep., Ala.)), available at 1997 WL 133277.

23. *Efforts to Fight Financial Crimes: Hearings Before the Subcomm. on General Oversight and Investigations of the House Comm. on Banking and Financial Serv.*, 105th Cong. (1997) (statement of Stanley Morris, Dir. FinCEN), available at 1997 WL 133277.

24. See *id.* (The CTR is the Currency Transaction Report that must be filed for every transaction in excess of \$10,000).

25. See Act of Oct. 26, 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified at 12 U.S.C. §§1951-1959 (1994)). See also John K. Villa, *A Critical View of Bank Secrecy Act Enforcement and the Money Laundering Statutes*, 37 CATH. U. L. REV.

be reported, in order to alert the law enforcement authorities to "suspicious" transactions that could be the initial step in the money laundering process. While it encountered controversy,²⁶ it has been upheld and is still applicable to specified financial institutions, and all individuals transporting in excess of \$10,000 into or out of the United States.²⁷ These requirements are now applicable to all non-banking financial institutions.²⁸

However, these regulations were inadequate to prevent money laundering, and the Money Laundering Control Act was passed. It "criminalized money laundering and structuring and provided for both civil and criminal forfeitures of funds or property implicated in the laundering."²⁹ The act of money laundering itself was now illegal. The MLCA also criminalized structuring, the process of breaking up large sums purposefully, so as to avoid the \$10,000 threshold for required reporting.³⁰ A part of the MLCA, the Right to Financial Privacy Act of 1978, gives banks limited protection for disclosing client information, in good faith, when there are signs of money laundering.³¹ In 1988, Congress enacted the Money Laundering Prosecution Improvements Act, which imposes liability and penalties on professionals who assist money launderers, including negligent bankers. This Act increased the cooperation between such professionals and their financial institutions and FinCEN.³² Finally, the Money Laundering Suppression Act of 1994 was enacted to reconcile growing differences among the various anti-money laundering statutes. It also streamlined the reporting

489, 491 (1988).

26. The Banking Secrecy Act was before the Supreme Court in *California Bankers Ass'n v. Schultz*, 416 U.S. 21 (1974) and *United States v. Miller*, 425 U.S. 435 (1976).

27. See 31 U.S.C. § 5312(a), (b) (1994); see also 31 C.F.R. § 103.22 (1997).

28. See Pub. L. No. 103-325, 108 Stat. 2243 (codified at 31 U.S.C. § 5330 (1994)); see also Barbot, *supra* note 2, at 186. The 1992 Annunzio-Wylie Anti-Money Laundering Act and the 1994 Money Laundering Suppression Act extended the reach of the Banking Secrecy Act, while guarding against undue reporting burdens on the financial institutions. *Id.* These Acts closed a significant loophole in the original Act, and brought all financial institutions under the same regulations designed to deter financial crimes. *Id.*

29. Sultzzer, *supra* note 2, at 158-159.

30. See *id.*

31. See Duncan E. Alford, *Anti-Money Laundering Regulations: A Burden on Financial Institutions*, 19 N.C. J. INT'L & COM. REG. 437, 459 (1994). (Without such protection, the bank would be liable to an innocent client for having reported them to government officials, and for having disclosed otherwise protected information).

32. See *id.* See also Lara W. Short, et al., *The Liability of Financial Institutions for Money Laundering*, 109 BANKING L.J. 46, 63-64 (1992).

requirement, so that the government can receive the information it needs to monitor financial crimes, but without subjecting the financial institutions to expensive reporting procedures or unreasonable liability.³³

The Electronic Funds Transfer Act (EFTA), and its enforcement mechanism, Regulation E, were passed as a first attempt at regulating the transfer of funds through an electronic medium.³⁴ This Act "establishes the basic rights, liabilities, and responsibilities of consumers who use electronic money transfer services, and of financial institutions that regulate these services."³⁵ Regulation E protects individual consumers, at the expense of the financial institutions. Currently, only Regulation E addresses "cyber-banking."³⁶

II. Challenges to Preventing Money Laundering Using Internet Casinos

The Internet provides individuals worldwide with the ability to communicate and exchange information across national boundaries and continents. The project to connect scientists and defense agencies has united the globe with access to information, available anywhere, at any time.³⁷ While facilitating commerce and communication, the Internet also facilitates the ability of criminals to elude the laws of any, and every, nation.³⁸ This "ethereal" Internet allows much cyber-crime, and with the advent of Internet gambling, the Internet now offers a technique to launder funds with unprecedented speed, ease and anonymity across international boundaries.³⁹ The Internet gambling industry is not insignificant. Revenues are projected at 25 billion dollars and are of concern to tax collectors and law enforcement internationally.⁴⁰ To succeed,

33. See Barbot, *supra* note 2, at 190-191, 218.

34. See Richard L. Field, *1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 AM. U. L. REV. 967, 975 (1997).

35. 12 C.F.R. §205.1(b) (1997); see also John K. Halvey, *The Virtual Marketplace*, 45 EMORY L. J. 959, 968 (1996).

36. See 12 C.F.R. § 205.6(b).

37. See *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), *aff'd*, 621 U.S. 844 (1997).

38. See Hogan, *supra* note 4, at 818-819.

39. See Marc S. Friedman & Kristin Bissinger, *Infojacking: Crimes on the Information Superhighway*, 9 NO. 5 J. PROPRIETARY RIGHTS 2, 2 (1997). See also Lawrence, *supra* note 8, at 4.

40. See *Internet Gambling Soon to Become a 25-billion-dollar Industry*, AGENCE FRANCE-PRESSE, Oct. 1, 1997, available at 1997 WL 13405120.

law enforcement needs cooperative efforts from the international community.

A. *Sovereignty and International Relations*

While there are myriad reasons to cooperate, universal international cooperation is an elusive goal. The Internet, because of its very nature as a network-based technology, requires multi-national oversight to provide effective enforcement. The Internet is not aligned with geography, and users have access to sites and information without regard for, or hindrance from, the territorial origin of that data.⁴¹ Consequently, so long as some jurisdictions are willing to allow Internet gambling sites, these virtual casinos are not subject to effective regulation by any one nation, or even a group of nations, because a site permitted in just one jurisdiction is accessible from all others. Large-scale laundering of criminal profits can only be prevented by broad jurisdictional cooperation. A partial success is no success at all, for it matters not to a would-be money launderer whether the site he relies on to launder his money is based in Antigua, Grenada or Liechtenstein.⁴² As long as there are nations willing to be host to on-line casinos, law enforcement officials worldwide will be fighting against stacked odds.

Effective prosecution of criminals requires international cooperation. While it is relatively simple to obtain evidence that on-line gambling has occurred, it is difficult to ascertain the size and scope of that gambling operation, and whether money is being laundered. Tracing a paper trail in an electronic environment requires the cooperation of foreign governments and is made increasingly difficult because of the complete anonymity of current cyber-banking and the increasing use of encryption technology, which obliterates the paper trail.⁴³ And, even when the evidence is

41. See Jonathan I. Edelstein, Note, *Anonymity and International Law Enforcement in Cyberspace*, 7 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 231, 237 (1996).

42. See *Minnesota v. Granite Gate Resorts, Inc.*, 568 N.W.2d 715, 717 (Minn. Ct. App. 1997) (discussing WagerNet's activities in Belize); Mark Fineman, 'Virtual Casinos' Cash in on Lax Rules in Antigua, LA TIMES, Sept. 21, 1997, at A1 (Antiguans are largely unaware of on-line gambling operations, even though they generate millions per month for operators; operators required to pay large licensing fees to government); Brett Pulley, *On Antigua, It's Sun, Sand and 1-800 Betting*, NY TIMES, Jan. 31, 1998 (Curacao hosts numerous bookie operations); Benjamin Weiser, *U.S. Charges 14 with On-line Sports Betting Operations*, NY TIMES, Mar. 5, 1998 (Antigua, Costa Rica and the Dominican Republic are home to such operations); *Betting Money on the Web*, NY TIMES, Mar. 5, 1998.

43. See Aaron Craig, *Gambling on the Internet*, 1998 COMP. L. REV. & TECH.

available, the prosecuting nation must rely on the existence of applicable extradition treaties or agreements, or extra-legal attempts to bring suspects within the prosecuting country's borders.⁴⁴ The notable lack of agreement further hinders crime-fighting efforts.⁴⁵ Finally, the legal costs of fighting venue/forum non conveniens, jurisdiction and notice for every trial are a significant deterrent to effective prosecution.⁴⁶

International cooperation is also suggested by other policy considerations. Individual nations also have an interest in protecting their own citizens from fraudulent on-line activities. International cooperation is necessary to develop secure connections for legitimate financial transactions. Without the ability to detect and monitor on-line gambling, no nation is able to protect its citizens from scam artists who have no intention of paying out winnings; nor is it possible to provide them with effective relief.⁴⁷

General international cooperation should generally benefit Internet commerce, as opposed to being only a regulatory burden. Professor Burk contends that "the prospect of states applying haphazard and uncoordinated multi-jurisdictional regulation to the Internet's seamless electronic web raises profound questions regarding the continued growth and usefulness of this medium"⁴⁸ Fragmented regulation leaves as the only options expensive or difficult compliance or shutting down.⁴⁹ The costs of redundant and contradictory regulations can deter the growth and expansion of commerce worldwide.⁵⁰ Such fragmentation might occur among the sovereign states within the United States. Notably, the Ninth Circuit has recognized that the Constitution's Commerce Clause guards against such consequences by discouraging "statutes that adversely affect interstate commerce by subjecting activities to inconsistent regulations."⁵¹ Uniform regula-

J. 61, 95 (1998).

44. See *id.* at 96.

45. See Friedman & Bissinger, *supra* note 39, at 9 (many computer crimes are not extraditable offenses).

46. See Craig, *supra* note 43, at 96.

47. See Hogan, *supra* note 4, at 856.

48. Dan L. Burk, *Jurisdiction in a World without Borders*, 1 VA. J. L. & TECH. 5 (1997).

49. See Hogan, *supra* note 4, at 844.

50. See *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1123 (W.D. Pa. 1997); John Gibeaut, *Questions of Authority*, 83 A.B.A.J. 42, 43 (1997) (quoting *Digital Equip. Corp. v. AltaVista Tech., Inc.*, 960 F. Supp. 456 (D. Mass. 1997)).

51. *Shell Oil Co. v. City of Santa Monica*, 830 F.2d 1052, 1058 (9th Cir. 1987).

tion is logical and, within the United States, supportable through Commerce Clause interpretations.

Currently, Internet casino operators are eschewing the United States for less restrictive jurisdictions, including Antigua, Belize, Costa Rica, Curacao, Dominican Republic, Grenada and Liechtenstein. These countries are preferable for Internet casinos, both because of their more favorable tax laws and their lack of applicable extradition treaties with the United States.⁵² Some host nations require the virtual casinos to pay a yearly licensing fee, or require that web sites post a bond with the local gaming commission to guarantee that winnings will be paid, or both. However, the amount of winnings distributed exceeds the amount of the bond within a few days of the casino's opening.⁵³ Some nations have even created a free trade zone, in which the Internet casinos can operate free from any corporate tax liability.⁵⁴

In the international arena, there are two additional "costs" associated with regulating Internet gambling operations. First, largely because of the implications of on-line casinos for funding criminal endeavors, national and international bodies are imposing on a traditionally local authority.⁵⁵ Second, if the United States wishes to enforce opposition to money laundering done through Internet casinos in other jurisdictions, the United States must assess the degree of cooperation from other jurisdictions and carefully weigh the cost attached to extradition and prosecution for violation of gambling laws. The doctrine of comity, which determines the degree of "recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience," will govern the expenditure of U.S. international political capital for such endeavors against the need to aggressively prosecute other on-line financial crimes⁵⁶

In sum, international cooperation is a prerequisite to any prevention of money laundering through Internet casinos. The

52. See Pulley, *supra* note 42 ("[o]f the approximately 60 offshore sports books in operation throughout the Caribbean and Central America, 25 are based in Antigua, according to local officials, who in 1994 created a free trade zone where the bookies can operate without paying corporate taxes.").

53. See Crist, *supra* note 3, at 88 (within minutes, the value of wagers placed exceed the bonds securing the winnings).

54. See *World Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980).

55. See Howard G. Zaharoff and Thomas W. Evans, *Cyberspace and the Internet: Law's Newest Frontier*, 41 BOST. B. J. 14, 14 (1997).

56. *Hilton v. Guyot*, 159 U.S. 113, 163-164 (1895).

technical complexities of the Internet make international cooperation among jurisdictions the threshold issue.

B. Jurisdictional Concerns

To prosecute money laundering through Internet casinos, some entity must have legal jurisdiction. Under the requirements put forth in *International Shoe Co. v. Washington*,⁵⁷ a court must find that the on-line casino has had sufficient contacts with the state in which the federal court is located so that bringing the on-line casino into that court is fair. Since the Internet gambling operation might not be considered to be physically present in the state, the court must find that a two-part inquiry into minimum contacts and fairness is satisfied,⁵⁸ such that the casino would have had "fair warning that a particular activity may subject [them] to the jurisdiction of a foreign sovereign."⁵⁹ The minimum contacts prong is satisfied if the casino has "purposefully directed" activities at the forum state.⁶⁰ This contact cannot be merely passive, but must be substantial enough⁶¹ to show that the casino has clearly enjoyed the privilege of doing business in the forum state.⁶² The fairness prong addresses whether it is reasonable to subject the casino to the jurisdiction of the court in the forum state.⁶³ The court must find either that it would be unfair to allow the casino to escape being brought before it, or that it was foreseeable that the casino would, at some point, be brought into that forum's court.⁶⁴ Consequently, a reasonable definition of contact could provide jurisdiction.

*In re DES Cases*⁶⁵ present an alternative means of gaining jurisdiction over Internet casinos. There the court held that it had jurisdiction over all of the hormone manufacturers, irrespective of any individual manufacturer's actual and specific connections with any particular state, because they had all introduced their products into the "national economic pond."⁶⁶ Under this ruling, personal

57. 326 U.S. 310 (1945).

58. See *Burnham v. Superior Ct.*, 495 U.S. 604, 618 (1990); *Pennoyer v. Neff*, 95 U.S. 714, 733 (1877).

59. *Shaffer v. Heitner*, 433 U.S. 186, 218 (1977) (Stevens, J., concurring); *Burger King Corp. v. Rudzewicz*, 471 U.S. 462 (1985); *World Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286 (1980).

60. See *Burger King*, 471 U.S. at 472.

61. See *McGee v. International Life Ins. Co.*, 355 U.S. 220, 223 (1957).

62. See *Burger King*, 471 U.S. at 476.

63. See *International Shoe*, 326 U.S. at 320.

64. See *World Wide Volkswagen*, 444 U.S. at 297; *Burger King*, 471 U.S. at 474.

65. *In re DES Cases*, 789 F. Supp. 552 (E.D.N.Y. 1992).

66. *Id.* at 589.

jurisdiction exists upon a showing of an "appreciable state interest."⁶⁷ It can be argued that the Internet is an economic pond, albeit a global one, because the individual web sites can be accessed from any other point around the world, and thus jurisdiction over Internet gambling sites is proper, provided that the forum state has an "appreciable interest" in the suit and that it is not unreasonable for the casino operators to defend the suit in that forum.⁶⁸

The application of this theory to the Internet was borne out in *CompuServe, Inc. v. Patterson*,⁶⁹ where the court held that the defendant's placement of goods into the stream of commerce (he sold goods via the Internet to Ohio residents) justified the Ohio court's jurisdiction over him. It appears obvious that an on-line casino is placing a product, the opportunity to gamble, into the stream of commerce. If the virtual casino allows the user to place a bet, then the forum state in which the user is located should be able to exercise jurisdiction over the Internet gambling operator.⁷⁰ A second Internet case, *Minnesota v. Granite Gate Resorts, Inc.*,⁷¹ established that the creation of a web site in one state was the equivalent of constantly broadcasting an advertisement with the same content at the residents of another state. This conclusion, plus evidence that residents in the recipient state called the toll free number provided, was adequate for the recipient state to have jurisdiction.⁷² There is, thus, precedent for not treating the Internet as *sui generis*. Rather, the Internet may be more akin to an electronic billboard, and therefore could be bound by all applicable media-neutral laws. The reasoning in this case would also support jurisdiction over an Internet casino once bets had been placed in a given jurisdiction.

However, the Internet gambling operators themselves may, through their own actions, provide the basis for jurisdiction. Before the on-line casino allows the individual gambler to place a bet, it will have taken many purposeful steps to ensure that, in the event the gambler loses, the casino gets its money.⁷³ While advertising

67. *Id.* at 587.

68. See Seth Gorman and Antony Loo, *Blackjack or Bust: Can U.S. Law Stop Internet Gambling?*, 16 LOY. L.A. ENT. L.J. 667, 684-685 (1996).

69. 89 F.3d 1257 (6th Cir. 1996).

70. See *id.*; *Burger King*, 471 U.S. 462 (1985).

71. No. C6-95-7227, 1996 WL 767431 (D. Minn. Dec. 11, 1996), *aff'd* 568 N.W.2d 715 (Minn. Ct. App. 1997).

72. See *Inset Systems, Inc. v. Instruction Set, Inc.*, 937 F. Supp. 161 (D. Conn. 1996).

73. See Bruce P. Keller, *The Game's the Same: Why Gambling in Cyberspace Violates Federal Law*, 108 YALE L.J. 1569, 1599 (May 1999).

and the mere "placement of a product into the stream of commerce, without more, is not an act of the defendant purposefully directed toward the forum State,"⁷⁴ once the gambler has released his credit card information to the on-line casino, and the casino has responded by sending over the Internet the multitude of images that constitutes the game being played, it is clear that there has been a purposeful directing of communication toward the forum state based on the responses of the Internet gambler.⁷⁵ The casino can argue that an individual gambler is not necessarily identifiable by geographic location.

United States case law, by analogy, supports a finding of jurisdiction over foreign subjects located in gambling-legal jurisdictions. As early as 1818, the courts had the authority to punish acts of piracy, even when the offending party was a foreigner.⁷⁶ More recently, the court supported the use of 18 U.S.C. 1084 as a means of prosecuting communications between the United States and offshore, gambling-legal jurisdictions to obtain jurisdiction over a party geographically located outside the United States.⁷⁷ The Supreme Court reiterated this message in *U.S. v. Fabrizio*,⁷⁸ when it held that when Congress enacted 18 U.S.C. 1084, it was aware of other nations' legal lotteries and did not include exceptions or exemptions. Therefore "even lawful state or foreign-based gambling operations properly were included within the scope of federal prohibitions."

In *Parke-Bernet Galleries, Inc. v. Franklyn*,⁷⁹ the court held that the defendant's conduct was sufficient to subject him to personal jurisdiction in the United States when he participated in an auction via telephone. This type of electronic transaction could be rationally analogized to an Internet communication. Other telephone cases have established that jurisdiction in the forum state cannot be evaded by conducting an illegal activity over the telephone in a jurisdiction where the activity is legal—the courts usually find that the foreign participation is virtually present in the forum state.⁸⁰ And, the Internet casinos' contacts with the United

74. *Asahi Metal Indus. Co. v. Superior Ct.*, 480 U.S. 102, 112 (1987).

75. *See State v. Rossbach*, 288 N.W. 2d 714 (Minn. 1980); Gorman & Loo, *supra* note 68, at 681-682.

76. *See U.S. v. Palmer*, 16 U.S. 610 (1818).

77. *See U.S. v. Blair*, 54 F.3d 639 (10th Cir. 1995).

78. *See* 385 U.S. 263 (1966).

79. 256 N.E.2d 506 (N.Y. App. Div. 1970).

80. *See PaineWebber Inc. v. Westgate Grp., Inc.*, 748 F. Supp. 115, 121 (S.D.N.Y. 1990); *Otterbourg, Steindler, Houston & Rosen P.C. v. Shreve City Apartments Ltd.*, 543 N.Y.S.2d 978 (App. Div. 1989); *China Union Lines v.*

States are usually not restricted to cyberspace alone; the virtual casinos' non-cyber contacts with U.S. citizens involve various other instrumentalities of interstate commerce, and thus the on-line casino operators have violated federal laws.⁸¹

The groundwork for the conclusion that 18 U.S.C. 1084 is lawfully applicable to Internet gambling prosecutions was laid in *U.S. v. Edge Broadcasting*.⁸² The Court acknowledged that Congress has broad powers under the Commerce Clause by upholding *Champion v. Ames*, and it upheld the validity of a federal gambling prosecution based, at least in part, on the prosecution of a gambling operation outside the United States in a jurisdiction that had legalized gambling. By harkening back to *Pensacola Telegraph v. Western Union Telegraph*,⁸³ the Court reiterated that Congress' Commerce Clause powers "are not confined to the instrumentalities of commerce . . . known or in use when the Constitution was adopted, but . . . keep pace with the progress of the country, and adapt themselves to the new developments of time and circumstance."⁸⁴ Certainly, the conclusion that the Internet is an instrumentality of interstate commerce is logical.

This series of cases would indicate that reasonably crafted federal regulation could obtain jurisdiction over Internet gambling activities that involve participants in, or are targeted at, the United States. Yet, such jurisdiction does not provide a complete solution. Once jurisdiction is established, actually securing the necessary information becomes the next significant hurdle to clear; a lack of international cooperation and technological barriers still hinder effective enforcement of existing laws. Also, restrictions on Internet activities must clear constitutional hurdles in the United States as well.

C. Balancing Individual Privacy and the Needs of Law Enforcement

The era of the Internet has only augmented the concerns for individual privacy, which have been escalating over the last half-century. Fighting crime has always required balancing constitutional rights of individuals against the need to detect and deter

American Marine Underwriters, 454 F. Supp. 198, 202 (S.D.N.Y. 1978).

81. See Keller, *supra* note 73, at 1601.

82. 509 U.S. 418 (1993).

83. 96 U.S. 1 (1877).

84. *Champion v. Ames*, 188 U.S. at 350 (1903), quoting *Pensacola Tel.*, 96 U.S. at 9.

criminal endeavors. The new technologies provide greater threats to privacy, but, ironically, can provide greater barriers to law enforcement's ability to collect vital information.

When a consumer wishes to make an on-line purchase, he typically opens an account with an electronic money issuer by purchasing tokens, coins or coupons, which are encoded data packets that represent an agreed-upon amount of currency. When the consumer makes the purchase from the merchant, the consumer downloads the tokens from his computer to that of the merchant, who then forwards the tokens to their issuer, who verifies them and credits the appropriate amount to the merchant's account.⁸⁵ While electronic money and the burgeoning e-commerce are quick and convenient, they implicate serious privacy concerns. Legitimate consumers and merchants need an Internet economic financial system that provides them with security, and that shields their personal information from prying eyes.⁸⁶

Counterbalancing legitimate privacy interests is the need for a trail, traceable by law enforcement, to ensure that the criminal elements do not have the privilege of committing crimes in undiscoverable anonymity.⁸⁷ Currently, "cyber-banking" allows the anonymous transfers of large sums of money, without triggering the reporting requirements that have proven effective in slowing the money laundering process.⁸⁸ By privately transferring funds on-line, criminals are able to bypass the traditional financial institutions with built-in procedures that discourage money laundering, and

85. See Michael A. Fixler, Note, *Cyberfinance: Regulating Banking on the Internet*, 47 CASE W. RES. L. REV. 81, 85-86 (1996); Catherine M. Downey, Comment, *The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?*, 14 J. MARSHALL J. COMPUTER & INFO. L. 303, 306-7 (1996); Ellen d'Alelio, *Doing Business in the New World of Electronic Commerce: An Introduction to the Emerging Electronic Payment Products and Systems*, DOING BUSINESS ON THE INTERNET 63, 70 (PLI Patents, Copyrights, Trademarks, and Literary Prop. Course Handbook Series PLI Order No. G4-4024, 1997).

86. See A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases*, 15 J.L. & COM. 395, 460 (1996); Henry H. Perritt, Jr., Legal and Technological Infrastructures for Electronic Payment Systems, 22 RUTGERS COMPUTER & TECH. L.J. 1, 3 (1996).

87. See Joshua B. Konvisser, Note, *Coins, Notes and Bits: The Case for Legal Tender on the Internet*, 10 HARV. J.L. & TECH. 321, 349 (1997); Nicholas W. Allard & David A. Kass, *Law and Order in Cyberspace: Washington Report*, 19 HASTINGS COMM. & ENT. L.J. 563, 605 (1997); Jonathan I. Edelstein, Note, *Anonymity and International Law Enforcement in Cyberspace*, 7 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 231, 255-63 (1996).

88. See Sultzer, *supra* note 2, at 195.

alert law enforcement officials to the possible commission of a crime.⁸⁹

An added difficulty in the privacy issues application across international boundaries is the difference between United States and European nations regarding the privacy of on-line information. The United States' Federal Bureau of Investigation is able to use "black box" surveillance systems that monitor and sort e-mail messages only after a search warrant is obtained.⁹⁰ In contrast, the British government is on the verge of passing new legislation that would allow the government to monitor electronic communications for a variety of reasons, including national security interests, the protection of the country's "well-being," and to detect and prevent serious crime.⁹¹ This legislation does not require that warrants for such monitoring come from judges; rather, a range of officials, including high-ranking police officials can sign them.⁹² Amnesty International in London has charged that this legislation "contravene[s] a large number of fundamental rights in the European convention on human rights and other international standards, which include the right to privacy, the right to liberty, the right to freedom of expression and the right to freedom of association."⁹³ While the British appear to have tipped the scales in favor of law enforcement, legitimate privacy concerns must be safeguarded, without jeopardizing law enforcement's ability to police effectively. Again, reaching an agreement for international cooperation will prove essential.

Traditional constitutional privacy hurdles would be raised if the British proposal was made in the United States. The test, as applied to privacy where it is construed as a fundamental right requires three steps. First, is there a reasonable expectation of privacy? Second, is there a compelling state interest? Third, if there is a compelling interest under reasonable expectation, was the regulation of the interest done in the least intrusive manner?

One could conclude that a rationally drafted measure monitoring Internet gambling could survive this test. First, an individual arguably may not have a reasonable expectation of privacy when gambling on the Internet. Further, the government

89. See John J. Byrne, *FATF Typologies Focus on Emerging Laundering Trends*, MONEY LAUNDERING L. REP., Aug. 1996 at 1, 4.

90. See Sarah Lyall, *British Authorities May Get Wide Power to Decode E-Mail*, N.Y. TIMES, INT'L at A3 (July 19, 2000).

91. See *id.*

92. See *id.*

93. *Id.*

could show a compelling interest in identifying money laundering activities at a place it occurs frequently: Internet casinos. Finally, a reporting requirement for identifying the size and scope of transactions would probably satisfy the reasonable requirement by being the least restrictive means of regulating this. Therefore, arguably legislation requiring information that should identify money laundering through Internet casinos could survive a constitutional privacy test.

III. Regulation and Enforcement: Gambling, the Internet and Dirty Money

The issues raised above necessitate creating an overall legal framework to control money laundering done through Internet gambling operations. First, it is essential to determine the ultimate objective of such legal changes; in other words, to establish whether the focus on preventing or regulating Internet gambling is done with the end goal of preventing money laundering.

A. *Regulation of Traditional Gambling Establishments*

Until 1976, the majority of the fifty states found the economic benefits of legalized gambling outweighed by the concomitant social ills.⁹⁴ Opponents of gambling argue that gambling increases crime, generates economic losses and diminishes morality. They further argue that gambling has historic ties to organized crime, and disproportionately harms the lower socio-economic strata.⁹⁵ Nonetheless, many communities have legalized gambling in pursuit of jobs and revenues.⁹⁶

Under the federal system of governance in the United States, the policy decisions relating to allowing or prohibiting gambling have generally been part of the states' constitutional police powers. In recognition of this division of authority, and the Tenth Amendment (according to its current interpretation), the 1976 Commission on the Review of the National Policy Toward Gambling proposed that the individual state governments decide the extent to which

94. See *Valley Broad. v. United States*, 107 F.3d 1328, 1331-32 (9th Cir. 1997), cert. denied 522 U.S. 1115 (1998); *Players Int'l v. United States*, 988 F. Supp. 497, 502 (D.N.J. 1997).

95. See JEROME SKOLNICK, *HOUSE OF CARDS* 101-118 (1978); Thomas L. Hazen, *Public Policy: Rational Investments, Speculation or Gambling? - Derivatives Securities and Financial Futures and their Effect on the Underlying Capital Markets*, 86 NW U. L. REV. 987, 1005 n. 91 (1992).

96. See Jon Bigness, *Companies Place Bets on Internet Gambling*, CHI. TRIB., Aug. 25, 1997, at 1, 4.

gambling would be legalized within their borders.⁹⁷ Until recently, this arrangement has proved largely satisfactory, as traditional gambling operations were confinable within the territorial bounds of their host state.⁹⁸

As counterpoint to the states' authority over the general welfare of their citizens, the national government has retained the power to regulate commerce among the states.⁹⁹ While the states generate the bulk of the regulations regarding gambling, Congress, under the aegis of its Commerce Clause powers, intercedes when the gambling in one state has a substantial affect on another.¹⁰⁰ Since 1827, Congress has exercised its authority to prevent one state from using means of interstate commerce to surmount the barriers against gambling erected by some, but not all, states.¹⁰¹ While these federal attempts at strengthening and protecting state laws regarding gambling have been subjected to numerous challenges, they have been uniformly upheld as legitimate expressions of Congress' Commerce Clause power.¹⁰² Even traditional gambling has been subject to federal jurisdiction under the Commerce Clause and the reach of federal authority appears even greater when the Internet is involved.

B. Internet Gambling Complications

The Commerce Clause prevents a state from implementing a policy that is national in scope or that "burdens" interstate commerce.¹⁰³ Previous attempts by states to protect local business interests at the expense of out-of-state commerce have been disallowed.¹⁰⁴

97. See 1976 Gambling Commission at 172.

98. See Stevie A. Kish, Note, *Betting on the Net: An Analysis of the Government's Role in Addressing Internet Gambling*, 51 FED. COMM. L.J. 449, 454 (1999).

99. See *id.* at 457.

100. See *id.*

101. See *United States v. Edge Broad. Co.*, 509 U.S. 418, 421 (1993).

102. See Keller, *supra* note 73, at 1584.

103. However, the Fourth Amendment does not require that a warrantless search be founded upon probable cause; *Terry v. Ohio*, 392 U.S. 1 (1968), held that reasonable suspicion may be sufficient.

103. See Kenneth D. Bassinger, Note, *Dormant Commerce Clause Limits on State Regulation of the Internet: The Transportation Analogy*, 32 GA. L. REV. 889, 920-22 (1998); David Post, *Gambling on Internet Laws*, AM. LAW., Sept. 1998, at 97 (the Dormant Commerce Clause requires national resolution of Internet gambling issues).

104. See *Bibb v. Navajo Freight Lines Inc.*, 359 U.S. 520 (1959) (Illinois was unable to require trucks passing through the state to use specially contoured mud

Recently, a New York federal district court considered the intersection of the Dormant Commerce Clause, state law and the Internet, and struck down New York's Internet Indecency Act,¹⁰⁵ which sought to prevent sexually explicit communications with a minor over the Internet. The court found "that the Internet is analogous to a highway or railroad," and that "the phrase 'information superhighway' . . . [is] more than a mere buzzword; it has legal significance, because the similarity between the Internet and more traditional instruments of interstate commerce leads to analysis under the Commerce Clause."¹⁰⁶ Of significance here is the court's conclusion that state-by-state regulation of the Internet "highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed."¹⁰⁷ In establishing that the Internet should be regulated at the federal, and not state, level, the court held that "the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether."¹⁰⁸

Federal and international authorities are the proper regulatory bodies for most Internet policies.¹⁰⁹ Not only does regulation at such levels side-step the Commerce Clause concerns, but the federal government is better able to fashion solutions that are acceptable to, and hence more likely to be enforced by, other sovereigns. On the practical level, the national government's financial and infrastructure support for the creation and rapid expansion of the Internet reinforces its regulatory authority.¹¹⁰ Most commentators agree that national and international regulation avoids one of the most costly consequences of redundant and conflicting regulation by each local power, the inability of Internet sites to comply, in a cost-effective manner, with the myriad fragmented rules and policies.¹¹¹

flaps); *Seaboard Air Line Ry. v. Blackwell*, 244 U.S. 310 (1917) (Georgia cannot require trains to stop and blow their whistles at every grade crossing in the state).

105. N.Y. Penal § 235.21(3) (McKinney 1998).

106. *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 161 (S.D.N.Y. 1997).

107. *See id.* at 168-169.

108. *See id.*

109. *See* Steven R. Salbu, Article, *Who Should Govern the Internet?: Monitoring and Supporting a New Frontier*, 11 HARV. J.L. & TECH. 429, 457 (1998).

110. *See id.*

111. *See id.* at 439, 458-459.

Irrespective of jurisdiction, the greatest difficulties occur when drafting an enforceable policy. The technology of the Internet and the international nature of its' use make regulation by states, or even nations, very difficult. The simplicity of Internet gambling makes regulation complex. Currently, it is easy and convenient to place an on-line bet. Any individual with access to the Internet can run a key word search, using a search engine, and, after selecting the web site that looks most promising, stare Lady Luck in the face, even if the on-line gambling provider is located in a host nation thousands of miles from that of the would-be gambler. New visitors to the site open an account, usually with a minimum deposit, before they begin placing bets or playing other games of chance. The site operators usually require that the account be funded from wired funds, money orders or with a credit card. When the gambler wins, he must trust that the on-line casino will indeed deposit his winnings in his account or send them to him by money order or wire transfer.¹¹²

The policy quandary is how to prevent Internet gambling from being used as a tool of money launderers without creating clumsy or unenforceable regulations governing Internet transactions. Clearly, some jurisdictions are willing and ready to accommodate Internet gambling, thus adding to the complexity of finding a workable solution. It must be asked whether it is possible to prevent money laundering through Internet casinos without the cooperation of every nation in the world.

While debating and drafting policies, agencies seeking to place limits on Internet gambling providers must carefully balance the desire of states and nations to collect revenue from this lucrative industry against both the traditional vices associated with gambling, and the new advantages that the Internet, and especially Internet gambling, offers to criminals.¹¹³ While on-line gambling will create jobs, the number will be relatively low, and the majority of new hires will be HTML and other computer programmers, who, arguably, could put their skills to better use.¹¹⁴ Moreover, although proponents of traditional gambling establishments can argue that the harms wrought by such easy access to games of chance are compensated for by revenue generated, in the on-line arena "private Internet gambling, in any form, will result in a net loss for

112. See Hogan, *supra* note 4, at 821-823.

113. See Craig, *supra* note 43, at 62.

114. See *id.* at 68-69.

the state.”¹¹⁵ Not only will Internet sites harm state lottery and pari-mutual endeavors, and their accompanying revenues, but the state, in all likelihood, will not be able to collect taxes on the Internet gambling revenues themselves, as the Internet gaming operators have already located themselves in more tax-friendly nations.¹¹⁶ At the same time, the ease and broad accessibility of on-line casinos will increase the number of gamblers, and correlatively, the number of gambling addicts, and thus place a further drain on the government.¹¹⁷

C. Old Game, New Location: Gambling On-Line May Be Illegal Now

While the technicalities of gambling differ significantly between the lavish gaming houses in Las Vegas and Atlantic City, and at the on-line gaming sites on the Internet, the act of gambling or wagering is the same. Gambling is an activity that should be unaffected, legally, by the medium in which it occurs; “for the purposes of federal antigambling laws, it is the 1990s equivalent of using the telephone to play the numbers or place bets.”¹¹⁸ The bottom line is that on-line gambling does not require a fundamentally new, or different, legal regime.¹¹⁹

The United States Attorney for the Southern District of New York believes that Internet gambling operators are in violation of federal antigambling laws, even when they have located their operations offshore, and has filed prosecutions against more than twenty Internet sports gambling sites, alleging that they are in violation of the Wire Wager Act.¹²⁰ The complaints filed contain descriptions of the “ubiquitous” contacts these sites have with U.S. citizens, as well as how the transactions between the site and U.S. citizens strongly parallel gambling transactions previously conducted over the telephone, or through the mail.¹²¹ In agreement with New York, Internet gambling should be considered as firmly

115. *Id.*

116. See ROBERT GOODMAN, *THE LUCK BUSINESS* 42-51 (1995); Nelson Rose, *The Legalization and Control of Casino Gambling*, 8 *FORDHAM URB. L. J.* 245, 245 n. 1 (1980).

117. See *id.*

118. See I. Trotter Hardy, *The Proper Legal Regime for “Cyberspace,”* 55 *U. PITT. L. REV.* 993-1000 (1994). Although some acts are unique to cyberspace, the “Internet presents no new legal issues when it is being used ‘simply [as] a medium of direct communication between people – much like the telephone, mail or fax.’”

119. See Keller, *supra* note 73, at 1573.

120. Keller, *supra* note 43, at 1574; 18 U.S.C. § 1084 (1994).

121. See *id.* at 1574.

within the purview of the federal government, and subject to the existing federal gambling regulations and prohibitions.¹²²

Upon a closer examination of the mechanics of Internet gambling, arguably it is merely a “new-media imitation” of that which has already been proscribed under federal law, and therefore, on-line gambling should be as tractable to the regulations that forbid gambling over the telephone, through the mail or by fax. These laws include the Interstate Wire Act,¹²³ the Travel Act,¹²⁴ and the Crime Control Act.¹²⁵

Of the applicable statutes to the Internet gambling operator, the Interstate Wire Act (IWA) has sparked the most interest because, in its breadth, it expressly prohibits the use of a wire transmission facility to carry on a gambling business.¹²⁶ Section (a) of the Act provides that “Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined under this title or imprisoned not more than two years, or both.”¹²⁷ Section (d) further provides that a common carrier who is “‘subject to the jurisdiction of the Federal Communications Commission’ can be compelled to discontinue, disconnect, or refuse service to any facility that is violating the Wire Act upon receiving notice of such violation from any federal, state, or local law enforcement agency.”¹²⁸

Internet casino operations are in violation of each of the four elements of the Act. The state must first establish that the Internet casinos are “in the business of” betting. In *United States v. Baborian*,¹²⁹ the court concluded that “any bookmaking operation that takes bets” is “engaged in the business of betting.” Under this generous definition, the on-line casinos that receive bets from

122. *See id.*

123. 18 U.S.C. § 1084 (1997).

124. 18 U.S.C. § 1952 (1997).

125. 18 U.S.C. § 1955 (1997).

126. *See Keller, supra* note 43, at 1580.

127. 18 U.S.C. § 1084(a) (1997).

128. 18 U.S.C. § 1084(d) (1997).

129. 528 F. Supp. 324, 328 (D.R.I. 1981).

gamblers satisfy this element. The second requirement is that the Internet casino "knowingly use a wire communication facility to transmit bets."¹³⁰ Under the IWA, any interstate use of telephone or telex lines for the transmission of gambling information is prohibited.¹³¹ The third element is that the Internet casinos use the Internet to transmit bets in interstate commerce; this is, by definition, satisfied so long as the casino operator receives bets from individuals in different states or nations.¹³² The final element requires that one of the two parties to the wager or bet, the Internet casino or the gambler, receive either money or credit from the outcome of the bet.¹³³ The nature of gambling is such that one party will win, and this requirement is satisfied regardless of which party is the winner.

The Interstate Wire Act prohibits more than just the placing and receiving of bets, however, and criminalizes the transmission of *any* information that makes it possible to place a bet.¹³⁴ It does not matter whether the bet is actually placed in a state or nation that allows that form of gambling. The House Report on this Act stressed that "nothing in the exemption, however, will permit the transmission of bets and wagers or money by wire as a result of a bet or wager from or to any State whether betting is legal in that state or not."¹³⁵ The conclusion to be drawn from this statement is that "the literal language of 1084 condemns all Internet transmissions to the United States of the digitized bits of information that create the virtual gambling site on a user's computer screen."¹³⁶ This act seems tailor-made to apply to Internet gambling.

However, the language of this Act appears self-contradictory. It places a specific prohibition on the transmission of "information assisting in the placing of bets or wagers on any sporting event or contest," as well as a more general prohibition against "the transmission in interstate or foreign commerce of bets or wagers" and "information assisting in the placing of bets or wagers."¹³⁷ While

130. 18 U.S.C. § 1084(a) (1997).

131. See I. Nelson Rose, *Gambling and the Law*, REPLAY MAG., 46, July 1995.

132. See *id.* at 46.

133. See 18 U.S.C. § 1084(a) (1997).

134. See Keller, *supra* note 73, at 1581.

135. H.R. REP. NO. 87-967 at 3 (1961), reprinted in 1961 U.S.C.C.A.N. 2631.

136. Keller, *supra* note 73, at 1582; see also *United States v. Reeder*, 614 F.2d 1179, 1184 (8th Cir. 1980).

137. 18 U.S.C. § 1084(a) (1997).

the argument can be made that this Act only applies to bets or wagers on sports-related events, it is a weak argument in light of the House and Senate Reports on the Act.¹³⁸ These reports reference "bets and wagers" without a sport-related limitation, and it is unlikely that Congress intentionally excluded the numbers racket from its prohibition.¹³⁹ Any confusion could be remedied by amendment, such as the proposed Internet Gambling Prohibition Act. This Act, despite any linguistic imprecision, "seems tailor-made for application to Internet gambling."¹⁴⁰

The Travel Act¹⁴¹ has also been used to prosecute organized gambling and may be well suited to Internet gambling operations as well.¹⁴² Under this Act, it is illegal to "travel in interstate or foreign commerce or use of the mail or any facility in interstate or foreign commerce with the intent to perform an unlawful activity, which includes any business enterprise involving gambling"¹⁴³

The court in *United States v. Lightfoot*¹⁴⁴ explained that the purpose of the Travel Act is to enable the federal government to prosecute members of organized crime and supply local law enforcement with federal assistance when fighting criminal activities that extend beyond the state borders.¹⁴⁵ Of importance to the Internet gambling debate is the conclusion that the court reached in *United States v. Smith*,¹⁴⁶ where it held that the Travel Act can be used to prosecute interstate gambling conducted over the telephone wires because the wires transmitted the data (the voices of the gamblers) in the same manner that physical goods are moved across the ground. The court found that the telephonic "voice packets" of gambling information violated the Travel Act. The Internet analogy is logical. The "transportation of data packets involving gambling information over the Internet is as clear a violation of the Travel Act as are the voices in *Smith*."¹⁴⁷

138. See H.R. REP. NO. 87-967, at 2-4 (1961), *reprinted in* 1961 U.S.C.C.A.N. 2631; S. REP. NO. 87-588, at 2-5 (1961).

139. See TIMOTHY L. O'BRIEN, *BAD BET: THE INSIDE STORY OF THE GLAMOUR, GLITZ, AND DANGER OF AMERICA'S GAMBLING INDUSTRY* 4 (1998).

140. Keller, *supra* note 73, at 1584.

141. 18 U.S.C. § 1952 (1997).

142. See Craig, *supra* note 43, at 81.

143. 18 U.S.C. § 1952 (1997).

144. 506 F.2d 238, 240-241 (D.C. Cir. 1974).

145. See *Lightfoot*, 506 F.2d at 240-241.

146. 209 F. Supp. 907, 916 (E.D. Ill. 1962).

147. Craig, *supra* note 43, at 82.

The Crime Control Act¹⁴⁸ provides a final illustration of applicable existing legislation. Congress has proscribed the operation of an “illegal gambling business” and broadly defines such as business as any gambling business that is in “violation of the law of a State . . . in which it is conducted,” that involves at least five people, and that “has been or remains in substantially continuous operation for a period in excess of thirty days or has a gross revenue of \$2000 in any single day.”¹⁴⁹

Significantly, the Crime Control Act does not necessitate a state court conviction of the casino operators.¹⁵⁰ In addition to the elements listed above, the only other requirement is that the gambling business violates some state law, “no matter how trivial.”¹⁵¹ The proof requirements associated with this Act are minimal; the government only has to prove that at least five people (not even the same five people), at all times during a thirty day period, conducted the illegal gambling activity.¹⁵² Moreover, the participation of these individuals does not have to relate to the actual gambling; it is sufficient that they are considered “necessary and helpful” to the operation.¹⁵³ The thirty day requirement will be satisfied if there is a “repeated pattern of gambling activity.”¹⁵⁴

These statutes seem adequately sweeping to ensnare the Internet gambling operators if they do business in the United States. The casino itself will have taken enough steps to knowingly engage in commercial transactions with United States citizens for jurisdiction to be clearly established. Further, legal authority under the previously mentioned acts may be sufficient to find criminal liability. Yet, the difficulty lies in discovering the illegal Internet gamble in the first place. The anonymity and secrecy surrounding the Internet, especially when money is involved, have presented unprecedented challenges to the law enforcement community worldwide. Finally, under the above laws, the casino, not the launderer, is the criminal. So, the goal to now be pursued, based on the above laws, is to shut down, or prevent, one means of money laundering where there is a connection to the United States.

148. 18 U.S.C. § 1955 (1994).

149. *Id.*

150. *See* United States v. Murray, 928 F.2d 1242, 1245 (1st Cir. 1991).

151. *See* 18 U.S.C. § 1955(b)(1) (1994).

152. *See id.*

153. *See* United States v. DiMuro, 540 F.2d 503, 508 (1st Cir. 1976), *cert. denied*, 429 U.S. 1038 (1977).

154. *See* United States v. Nerone, 563 F.2d 836, 843 (7th Cir. 1977); United States v. Allen, 588 F.2d 1100, 1104 (5th Cir. 1979), *cert. denied*, 441 U.S. 965 (1979).

IV. The Advantages of New Legislation

A. The Internet Gambling Prohibition Act: Promises and Problems

Congress, seeking to make certain that Internet gambling is illegal, considered specific legislation this year. In the 106th Congress, both the Senate and the House of Representatives considered a version of the Internet Gambling Prohibition Act of 1999.¹⁵⁵ This proposed amendment to the Interstate Wire Act¹⁵⁶ would have made it "unlawful for any person engaged in a gambling business to knowingly use the Internet or any other interactive computer service to: (1) place, receive or otherwise make a bet or wager; or (2) send, receive, or invite information assisting in the placing of a bet or wager."¹⁵⁷ The amendment would change the Interstate Wire Act in two important ways. First, it would remove the limiting language in the Wire Act that criminalizes only the use of interstate wire communication facilities for sports betting, and create a much broader federal prohibition against almost any form of Internet gambling.¹⁵⁸ Second, the amendment would authorize federal law enforcement officials to seek injunctive relief against any Internet service provider who knowingly receives or transmits either a bet or wager, or information that assists in placing a bet or wager.¹⁵⁹

Although the bill is championed by some as the best solution to the growing Internet gambling industry, there are several criticisms of this particular proposal. While the amendment carved out exceptions for certain State lotteries and authorized horse and dog racing, critics of the bill said that it infringed on states' rights by preventing state lotteries from offering in-state sales of lottery tickets over the Internet.¹⁶⁰ Rep. Patrick Kennedy, D-R.I., appeared relieved that the bill failed, as it did not provide adequate protection to state lotteries, which he considered "perhaps the best form of gambling we have out there, in that they are giving legitimate dollars to our states."¹⁶¹

155. See H.R. 3125, 106th Cong. (1999); S. 692, 106th Cong. (1999).

156. 18 U.S.C. § 1084 (1997).

157. Internet Gambling Prohibition Act of 1999, H.R. 3125, 106th Congress (1999).

158. See H.R. 3125, *supra* note 155.

159. See *id.*

160. See *id.*

161. *House Deals E-gambling Bill Losing Hand*, ASSOCIATED PRESS (July 18, 2000).

Another issue is that the Supreme Court's recent decision in *Reno v. ACLU*¹⁶² raises First Amendment concerns regarding a federal ban on Internet gambling.¹⁶³ Under the current version of the Internet Gambling Prohibition Act of 1999, states would not be allowed to permit their citizens to gamble over the Internet even if all transactions occurred entirely intrastate.¹⁶⁴ However, the language in *Reno* may indicate that Congress cannot treat Internet gambling as "merely a vice activity that is undeserving of any First Amendment protection,"¹⁶⁵ and thus, some argue that a complete ban on all wagering activities over the Internet might not withstand a constitutional challenge. However, the Interstate Wire Act already permits law enforcement authorities to compel common carriers to discontinue service to any facility whose service is used for "the purpose of transmitting or receiving gambling information in interstate or foreign commerce in violation of federal, state or local law"¹⁶⁶ Since 1961, the courts have upheld this section of the statute against all constitutional challenges. As currently written, the Internet Gambling Prohibition Act of 1999 would merely extend the reach of the Interstate Wire Act to include the "interactive computer service provider[s]."¹⁶⁷

A final comment regarding any new proposals is relevant. Without the means to monitor, detect and prevent illegal transactions, i.e. without effective enforcement, these new laws would be merely a national moral proclamation.

B. Reporting Requirements: Detection and Deterrence

Under current technologies, it is impossible to register a domain name or set up a Web site anonymously.¹⁶⁸ Money, the root of the problem with on-line gambling operations, is, ironically, the saving grace; the registration services and Internet service providers require reliable billing information in exchange for their services.¹⁶⁹ This billing information connects a cyberspace entity with a concrete, geographical existence, and provides law enforcement

162. *Reno v. ACLU*, 521 U.S. 844 (1997).

163. *See id.*

164. H.R. 3125, *supra* note 155.

165. *See Reno v. ACLU*, 521 U.S. 844 (1997); Kish, *supra* note 98, at 451.

166. 18 U.S.C. § 1084(d) (1997).

167. H.R. 3125, *supra* note 155.

168. *See Keller*, *supra* note 73, at 1606.

169. *See id.*; *see, generally*, Network Solutions, Inc.'s Domain Name Registration Policies. The name, address, phone, fax and e-mail address of an "administrative contact" is required from each registrant.

with the beginning of a paper trail. These "footprints" make the Internet gambling operators susceptible to traditional law enforcement investigations and prosecutions, including sting operations and sham accounts opened by undercover operatives.¹⁷⁰ As one writer succinctly put it: "Always follow the money."¹⁷¹

To maximize efficiency, a federal agency could be charged with creating and maintaining a "Master List" of all web sites known for or suspected of permitting on-line wagering.¹⁷² Search engines and indices are effective tools for discovering these operations, as the operators need customers in order to survive and are thus locatable to those searching.¹⁷³ After searching for illicit gambling web sites, law enforcement authorities can require service providers to provide the identifying information they have, and the authorities have the option of following the paper trail and prosecuting on the basis of available information, or they can direct the service provider to block access to that site, thus shutting down the criminal operation. Both options, however, require international cooperation if Internet gambling operations are not to be available to criminals for large-scale money laundering.

Fortunately, law enforcement investigators and investigative technologies have not fallen behind the criminals.¹⁷⁴ The FBI and state law enforcement have conducted joint sting operations on the Internet that have generated sufficient evidence to arrest dozens of on-line wrong-doers.¹⁷⁵ State attorneys general offices, the Securities Exchange Commission and the Federal Trade Commission have also been successful in monitoring and prosecuting Internet fraud schemes.¹⁷⁶ These investigative forces have proven that law enforcement is able, and determined, to remain abreast of the emerging sophisticated technologies, in order to apply the law

170. See Dominic Bencivenga, *Internet Cyberforce: SEC and FTC Crack Down on On-line Fraud*, N.Y. L. J., Sept. 3, 1998, at 5; David Johnston, *Use of Computer Network for Child Sex Sets off Raid*, N.Y. TIMES, Sept. 14, 1995, at A1.

171. See Bencivenga, *supra* note 170, at 5.

172. See Craig, *supra* note 43, at 96.

173. See *id.*

174. See, generally, Johnston, *supra* note 170.

175. See Christopher Wolf & Scott Shorr, *Cybercops are Cracking Down on Internet Fraud*, NAT'L L. J., Jan. 13, 1997, at B12. (Here, the agents successfully posed on-line as minors, and were able to arrest dozens of on-line child pornographers).

176. See Bencivenga, *supra* note 170, at 5 (The SEC employs over 100 attorneys, analysts and accountants who are specially trained to detect and investigate cyber-crime. The FTC has similarly trained over 300); Wolf & Shorr, *supra* note 175, at B12.

to all criminals.¹⁷⁷ Money launderers using the Internet are still real people, with “real names, real addresses and telephone numbers and they want their money”¹⁷⁸ Since the act of laundering money is itself illegal, and since illegally acquired proceeds are always illegal, following the money is still a smart policy for crime prevention.¹⁷⁹

V. Conclusory Thoughts and Options

In the United States, citizens have a right to privacy interpreted from the federal Constitution, as well as some state constitutions against government intrusion. To their advantage, they are able to enjoy the rights provided by whichever source provides the better protection. In Florida, one of the most generous states, vis a vis a right to privacy, the test, the same basin test used for the federal fundamental rights, is: (1) In this setting, or for this activity, is there a reasonable expectation of privacy? (2) In this setting, or for this activity, does the state have a compelling interest in monitoring, regulating or limiting it? and (3) Was the government’s means the least intrusive available?

When applied to the Internet, citizens would appear to have a right to privacy against government intrusion. However, whether there is a compelling state interest depends on the actual circumstances. For example, the government has a proven interest in prosecuting child pornographers that use the Internet to ensnare unwitting victims. In large measure, the government’s interest in regulating activities on the Internet parallel their interest in those same activities when they are conducted in the “real” world.

The government has maintained a high level of regulatory interest in and control over the gambling industry in the United States. The casinos are monitored for fairness, as well as to prevent money laundering. The streets around the casinos are patrolled in order to prevent derivative crimes. There exists a compelling state interest in regulating the gambling industry. This interest does not diminish when the gambling occurs over the Internet; in fact, the government’s concerns are magnified. The government has a fully justified interest in preventing the on-line casinos from becoming the conduit through which millions, and perhaps, if not checked, billions, of dollars are laundered.

177. See Keller, *supra* note 73, at 1607.

178. Bencivenga, *supra* note 170, at 5, quoting Jodie Bernstein, Director, FTC Bureau of Consumer Protection.

179. See *id.*

Although only one of the three prongs of the privacy test must be satisfied in order for the state to lose a privacy test with respect to a given activity, Internet gambling should fail all prongs. There is no reasonable expectation of privacy when a gambler enters a casino in Las Vegas or Atlantic City. The ceiling is teeming with hidden cameras and the casino floor supports many employee-observers. Both the casino and the government take steps to monitor the patrons and the goings-on in a gambling institution. Since the same activity occurs on-line, the same justifications exist for monitoring the actions of the house and the gambler, and may be even stronger, based on money laundering activities.

The activity of on-line gambling cannot satisfy any part of the privacy test; there is not a reasonable expectation of privacy when gambling, and the state should have a compelling interest in preventing money laundering and other financial crimes. So long as the regulations are least intrusive, they are constitutional. In light of this, so long as any gambling sites are accessible on the World Wide Web, the government should be granted the ability to reasonably monitor Internet casino sites and to compel disclosure paralleling the non-Internet environment.

VI. The Constitution and Human Rights

A. *The Privacy Conundrum*

An overview of privacy concerns relating to the emerging world of cyber finance reveals the quandary facing policy makers. Private citizens wishing to engage in commercial transactions over the Internet need a secure communication format that prevents third parties from viewing their sensitive personal financial information without their consent. These third parties include would-be criminals and over-zealous marketers, as well as the government. Without a guarantee of a minimum modicum of privacy, the rapid expansion of Internet commerce will be slowed. On-line merchants have recognized this and most of the larger retailers doing business on the Internet have a privacy or security statement designed to reassure users that any financial or personal information released to the site will remain confidential.

When a consumer wishes to make an on-line purchase, he typically opens an account with an electronic money issuer by purchasing tokens, coins or coupons, which are encoded data packets that represent an agreed upon amount of currency. When the consumer makes the purchase from the merchant, the consumer

downloads the tokens from his computer to that of the merchant, who then forwards the tokens to their issuer, who verifies them and credits the appropriate amount to the merchant's account.¹⁸⁰ While electronic money and the burgeoning e-commerce are quick and convenient, they implicate serious privacy concerns. Legitimate consumers and merchants need an Internet economic financial system that provides them with security, and that shields their personal information from prying eyes.¹⁸¹

As counterpoint to the consumers' insistence on security in on-line financial transactions, the law enforcement community has an equally legitimate need for information in order to carry out their mandate to detect, deter and prosecute crimes. In the "real" world, most transactions leave a "trail," usually made of paper. When a money launderer begins to churn his illegal profits, there is often a record of the funds entering one business or account, and another showing where it was deposited after being removed. The process of layering may be confusing and tangled, but there is frequently a record of the events. The era of the Internet has only augmented the concerns for individual privacy, which have been escalating over the last half-century. Fighting crime has always required balancing constitutional rights of individuals against the need to detect and deter criminal endeavors. The new technologies provide greater threats to privacy, but, ironically, can provide greater barriers to law enforcement's ability to collect vital information.

Currently, "cyber-banking" allows the anonymous transfers of large sums of money, without triggering the reporting requirements that have proven effective in slowing the money laundering process.¹⁸² By transferring funds on-line, criminals are able to bypass the traditional financial institutions that have built-in procedures that discourage money laundering, and alert law enforcement officials to the possible commission of a crime.¹⁸³

On the Internet, however, it is possible to conduct business in complete anonymity. While this may be an attractive feature to libertarians, one must ask whether such complete secrecy benefits anyone other than criminals. In light of the unprecedented magnitude of on-line money laundering, especially through Internet gambling operations, the anonymity that is currently possible only

180. See Bryan S. Schultz, *Electronic Money, Internet Commerce, and the Right to Financial Privacy: A Call for New Federal Guidelines*, 67 U. CIN. L. REV. 779, 785 (1999).

181. See *id.*

182. See Sultzter, *supra* note 2, at 195.

183. See Byrne, *supra* note 89, at 4.

on the Internet may not be desirable. While security and privacy features must exist in order to promote cyber commerce, there is a compelling argument against allowing any more heightened features than currently exist and are used for similar transactions in the paper world.

While such a proposal to limit the security and degree of anonymity available on the Internet will be controversial, it is obvious that while many law-abiding individuals may wish to hide in cyberspace, it is only the criminals who have the most to lose by such a provision, as they will no longer be able to completely hide their actions from the light of day.

Compounding the situation are the fundamental differences that currently exist between the United States and European nations regarding the privacy of on-line information. The United States' Federal Bureau of Investigation is able to use "black box" surveillance systems that monitor and sort e-mail messages only after a search warrant is obtained.¹⁸⁴ However, the British government is on the verge of passing new legislation that would allow the government to monitor electronic communications for a variety of reasons, including national security interests, the protection of the country's "well-being," and to detect and prevent serious crime.¹⁸⁵ However, this legislation does not require that warrants for such monitoring come from judges; rather, they can be signed by a range of officials, including high-ranking police officials.¹⁸⁶ Amnesty International in London has charged that this legislation "contravene[s] a large number of fundamental rights in the European convention on human rights and other international standards, which include the right to privacy, the right to liberty, the right to freedom of expression and the right to freedom of association."¹⁸⁷ While the British appear to have tipped the scales in favor of law enforcement, legitimate privacy concerns must be safeguarded, without jeopardizing law enforcement's ability to police effectively. Again, reaching an agreement for international cooperation will prove essential, and probably just as elusive.

B. Freedom of Expression

In addition to the concerns of the right to privacy, the individual's freedom of expression may be implicated as well. The

184. See Lyall, *supra* note 90, at A3.

185. See *id.*

186. See *id.*

187. See *id.*

availability of other “vices” on-line have been the targets of regulation. An example of regulation of national and international Internet commerce, which failed constitutional muster, is the Communications Decency Act of 1996. The United States Supreme Court held that the Act was unconstitutionally vague, failed to use the least intrusive means to regulate child pornography on the Internet, and thereby violated the First Amendment’s Freedom of Speech.

The characteristics of the Internet were critical to the Court’s holding. The Court acknowledged that the Internet is unique.¹⁸⁸ No single organization controls the web, nor is there a centralized point to block communications.¹⁸⁹ It is currently impossible to determine the identity or authoritative information of a user of a site without requesting the information from that party.¹⁹⁰

The current conclusion that speech on the Internet is *more* protected than either radio or television airwaves, which are publicly regulated.¹⁹¹ Regulation of mass communication is medium specific and the Internet is the most participatory form of mass speech yet developed, and is entitled to the “highest protection from governmental intrusion.”¹⁹² Currently restrictions on Internet vices can fail constitutional tests.

C. 4th Amendment Concerns

A final concern that must be addressed before solutions can be sought and policies implemented is that of the constitutional protection against “unreasonable searches and seizures”; this safeguard requires that “no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”¹⁹³ In the context of money laundering through Internet casinos, the primary issue is not whether the law enforcement agencies are technologically capable of engaging in surveillance of such on-line entities, but when, and under what circumstances, may they legally monitor the presumably legitimate transactions of a legal business.¹⁹⁴

188. See *Reno*, 521 U.S. at 9.

189. See *id* at 10.

190. See *id* at 12.

191. See *id* at Syllabus 6.

192. See *id* at 17.

193. U.S. CONST. amend IV (1791).

194. It is critical to this analysis to note that, as previously stated, almost all on-line casinos are registered and operated from outside the jurisdictional boundaries

In general, a warrant is required before a search occurs, unless there are “exigent circumstances,” and any such search must not be “unreasonable.” The Fourth Amendment requires that before a judge or magistrate may issue a search warrant, he must be satisfied that probable cause to do so exists. The warrant must contain a particular description of the premises to be searched and the things to be seized. The Supreme Court has held that probable cause must also exist before a warrantless search is made. For there to be probable cause to search particular premises, “it must be more likely than not that (a) the specific items to be searched for are connected with criminal activities, and (b) these items will be found in the place to be searched.” Moreover, searches may be made of the premises of persons who are not themselves criminal suspects, if the law enforcement official, judge or magistrate has probable cause to believe that the search will produce evidence of another individual’s crime.¹⁹⁵

Health and safety inspections provide a parallel to the inspections that law enforcement personnel would be interested in conducting in the virtual casinos. The Supreme Court announced the general rule in *Camara v. Municipal Court of the City and County of San Francisco*,¹⁹⁶ that a search warrant is required before an inspector can conduct a health or safety inspection. But, in order to get a warrant for such an inspection, the inspector does not have to have probable cause that a violation will be discovered during the investigation; he must only show that the inspection is part of a “general area” inspection and that these premises are not being singled out. However, if a business is subject to special stringent licensing rules, a warrantless search/inspection may be allowed. For example, weapons dealers can be searched without a warrant because the federal government requires a license for all such dealers. This could be of particular value to law enforcement officials seeking to monitor on-line casinos for money laundering transactions if the legislature were to pass such “special stringent” licensing rules.

of the United States. While it may indeed be possible to find that the U.S. has jurisdiction over a particular web site that has engaged in repeated information transfers with a citizen of the U.S., these offshore companies are not, in general, subject to U.S. laws.

195. This will be especially useful in the on-line casino context, as the casino may not have any role in the laundering of money, but may be an unwitting and unknowing pawn.

196. 387 U.S. 523 (1967).

Before the probable cause analysis can begin, there must first be a statute that is potentially being violated. With an on-line casino, there are several possibilities, but they are predicated upon a finding that the business is subject to U.S. laws. Its operations could well be in violation of the Wire Act or federal reporting requirements, or it could be engaged in, or being used as a conduit for, money laundering or other such obvious criminal endeavors. If the law enforcement officials have a reasonable suspicion that the web site operator is in violation of an applicable law, or is being used to facilitate the commission of a crime, then they may be able to begin observing the business for further evidence of a violation. However, since the transactions with this enterprise are all on-line, observation is much more complicated, legally and practically, than setting up an observer across the street. In order to actually gain useful information regarding the possible criminal activities of an on-line casino, law enforcement would need to either observe each transaction and discover the identity of the transacting parties, or gain access to the casino's record books. While it is no doubt technically possible for the government to monitor all transactions the business engages in, Professor Baldwin reiterates emphatically that it is not legal under U.S. law to monitor a lawful business for compliance with a reporting requirement, which is the most probable and easily detectable of the potential criminal violations an on-line casino would commit. The only legal means of monitoring a business' transactions is to first find probable cause that the business is engaging in illegal activities and to obtain a search warrant from a judge or magistrate. Moreover, the technological resources available from Carnivore are not available here because that program is authorized only to investigate suspicious e-mails.

A final note of importance is that the Kyle amendment, which would enable law enforcement to search and monitor for exactly such money laundering threats, has been defeated every time it has been brought before the U.S. Congress for a vote.

VII. Options and Alternative Solutions

A. National Remedies and Limitations

In the battle against money laundering through the Internet, there is the tremendous burden of coping with the fact that these crimes are being committed on a world wide web, and hence, have instantaneous global implications. But even with the lack of

boundary lines on the Internet, the tendency may be for countries to attempt to eradicate the problem within their own boundaries. For example, while in Belgium and Denmark there are no specific regulations regarding the dissemination of information relating to securities on the Internet, in Sweden the Marketing Act sets regulatory standards for all marketing regardless of media and product.¹⁹⁷ It is these wide range of diverging regulations that serve to open the door for criminals to pick and choose the best arenas to facilitate their crimes.

It is not realistic to expect one nation to eliminate a worldwide problem. The Securities Exchange Commission in the United States acknowledged this fact in 1998 when it issued the "Internet Release."¹⁹⁸ Even though in 1999 alone, the SEC Division of Enforcement doubled the size of its Internet surveillance team, Cyberforce, from 125 to 250, and has been coordinating with the FBI, CIA, the FTC, and the Secret Service in an effort to curb fraud over the Internet,¹⁹⁹ the SEC still acknowledged that, as a "practical matter," forcing all offshore on-line securities service providers to register with the SEC would not be possible.²⁰⁰ The approach of the SEC is that unless the Internet solicitation and offers on the Internet are not "targeted" to the United States, then they are beyond the boundaries of what they choose to be SEC enforcement.²⁰¹ If a company takes measures to guard against sales in the United States, then they are free from SEC enforcement.²⁰² In fact, it is "well recognized" that the Securities Exchange Act is silent as to extraterritorial application.²⁰³

The SEC stance is that, "absent the transaction of business in the United States or with U.S. persons, our interest in regulating solicitation activity is less compelling."²⁰⁴ The SEC believes its focus should be to encourage issuers of securities and financial service

197. See Nelson, *Securities Law and the Internet: An International Perspective on E-Commerce*, 1188 PLI/Corp 449, 503-504 (2000). Additional examples of countries with minimal or nonexistent regulations on business's use of the Internet are Australia, Ireland, Greece, and The Netherlands. See *Id.*

198. See Securities Act Release No. 7516 (Mar. 23, 1998) [hereinafter Internet Release].

199. See Quinn, *Securities Regulation and the Use of Electronic Media*, 1188 PLI/Corp 315, 349 (2000).

200. See Statement of the Commission Regarding Use of Internet Web Sites to Offer Securities, Solicit Securities Transactions or Advertise Investment Services Offshore, 1189 PLI/Corp 131, 135 (2000).

201. See Securities Act Release No. 7516 at 14807.

202. See *id.*

203. *Itoba Ltd. v. LEP Group PLC*, 54 F.3d 118, 121 (2d Cir. 1995).

204. Securities Act Release No. 7516 at 14808.

providers to implement precautionary measures that are reasonably designed to ensure that offshore Internet offers are not targeted to persons in the United States or to U.S. persons.²⁰⁵ However, in an attempt to draw this parallel to curbing money laundering on the Internet, the shortcomings become very obvious very quickly.

If a country such as the United States were to take this isolationist point of view in the area of Internet gambling, it would do little to curb the abuses worldwide. Granted, perhaps fewer citizens in the United States would be involved, and Internet gambling sites would be more hesitant to solicit business from people in the U.S. But this decision would just allow for a company to set up sites, as has already occurred in Caribbean nations, and permit accomplices to place bets laundering money from Canada.

While the SEC has chosen to not police securities fraud offshore, the need to eliminate money laundering through the Internet is compelling. As is demonstrated by the varying degrees of enforcement that many countries currently have in the securities regulation department, unless an international agreement is reached, there will continue to be avenues of escape and loopholes for the criminals of this world. While it is admirable that one nation is willing to take steps to curb abuses in their own land, in the broader scheme of things, these measures are insufficient. As the Chairman of the Financial Services Authority of the United Kingdom, Howard Davies, stated quite succinctly at his speech at the Labour Party Conference of September 28, 1999, "we have to find a way of adapting our regulatory environment to new technology, not adapting the new technology to the old regulatory rules."²⁰⁶ In other words, the United States should not retreat to its' own borders in seeking to prevent money laundering. Consequently, seeking international cooperation is central to the success of the effort to prevent money laundering.

B. International Cooperation—Treaties

If we are to eradicate or deter the problem of money laundering via Internet gambling, there must be an international consensus on the proper means of reaching the goal. Because we

205. *See id.* Examples that the SEC envisions are the issuer's website including a prominent and meaningful disclaimer making it clear that the offer is directed only to countries other than the United States, or even going a step further and taking measures to ensure that sales are not made to people in the U.S. by blocking access to the offering materials.

206. Nelson, *supra* note 194, at 488.

are dealing with the 'world-wide-web', a worldwide solution is essential. The quandary arises, however, as to what exactly this worldwide solution is going to be.

The first necessary step to officially proclaiming international cooperation is a treaty. All members of the United Nations should participate in an agreement that embodies the desired goal and contains a means of enforcing this goal. Under the U.N. treaty, an international police system would be instituted so that there would be constant monitoring on the Internet to detect gambling sites that were operating, and then pinpointing their location and taking the necessary action provided for by the law. With the countries of the U.N. bound together by treaty, their resources can be pooled, thereby making it easier and more efficient to coordinate law enforcement activities and personnel.

If the goal is to prosecute individual on-line gamblers, U.S. law currently exists that allows prosecution of both the gambler and the Internet casino. However, if the primary objective is to prevent on-line casinos from being used as a conduit for laundering large sums of illegally acquired profits, then laws that allow the government to prosecute individual gamblers are of little value unless the government can effectively track the gamblers who are also money launderers. But as previously noted, the global nature of the Internet will allow an individual anywhere in the world to access a web site, and thus bypass any connection to just one nation. Without a connection to a particular nation with a strong commitment to defeating money laundering schemes, the transaction may be beyond the reach of prosecutors. This is where an international treaty that emphasizes a commitment to preventing and prosecuting money launderers, wherever found, and wherever based, becomes of paramount importance. In order to detect, and then prosecute, money laundering through on-line casinos, the law enforcement must be able to either monitor the businesses for suspicious transactions, or periodically review their financial records for such transactions. While this function is undoubtedly possible technologically, it must also be done legally, so that the evidence can be the foundation of a conviction.

Thus, the international community should give priority to strengthening anti-money laundering laws and to enabling international crime fighting agencies to effectively pursue evidence against such activities. There should be a strong commitment to sharing information and to facilitating extradition in order to make the most effective use of the limited resources available for such operations. Additionally, it must be remembered that in the end, at

least one nation must have legal jurisdiction over the criminals and must be able to arrest and prosecute them. The international treaties should be designed with teeth sufficient to deter criminal endeavors, but must also be cognizant of the particularities of jurisdiction and due process so that evidence gathered will be admissible.

C. Complete Ban vs. Licensing and Regulation

There are essentially two philosophies one can abide by in an attempt to solve the problem. The first is to completely ban all internet gambling sites. If there is not a means for which to launder the money by, then the possibility of money laundering through the internet will be unavailable to the criminal. A second approach is to allow internet gambling sites to operate, but requiring all sites in operation, and all future sites to register and become licensed to operate. This would enable law enforcement authorities to keep tabs on the sites that are legally registered, and would also assist them in detecting those sites that are operating without a license. Could the United States require sites to register and report activity related to the United States? Probably, yes.

The problem then becomes how to stop these sites from springing up anywhere in the world where a computer can be connected and a phone line exists. Therefore the overall feasibility of eliminating all gambling sites necessarily dictates a strong consideration of the second option, licensing and regulation. Arguably licensing is a more realistic approach, both in terms of implementation and enforcement. But again, transnational cooperation would be essential. Therefore under a licensing arrangement, if these pirate sites were to spring up, they would be more easily detectable because they could be identified as unregistered and flagged for lack of certification.

D. General Surveillance vs. Target Approach

Whichever tactic is eventually implemented, there must be a means of enforcing the rule of law. Inextricably tied to the registration approach is the strategy of general surveillance. Under this method, the required registration could mandate lists of all members who are gambling on the companies' sites, as well as continuous reports of their transactions. A more limited approach would be to require reporting of significant transaction and the identity of those involved. While privacy concerns may be implicated, a compelling government interest should justify such an

approach in gambling if the least intrusive means were used. If, through general surveillance, law enforcement has reason to inspect further, based on either large transactions or suspicious transfer of funds, a more specified approach would then be taken toward the possible wrongdoer, who might then become a target of an investigation.

While the general surveillance approach has its merits in that all gambling sites licensed could be monitored, its detractors warrant considering a more targeted philosophy from the outset. Under general surveillance, an administrative nightmare may be created, with all figures constantly flooding the regulatory agency, and law enforcement officials being required to keep abreast of each company and their unusual transactions. Under a more targeted approach, spot checks could be made into the various companies. A greater emphasis would be placed on underground information so as to hone in on those sites that are believed to be laundering money. Additionally, greater constitutional justification will likely exist under this approach, because with information of suspicious activity and the opportunity for a more detailed probe into the numbers of one specific company, probable cause would be required when the initial action is taken.

E. Agreement, Then Action

From international cooperation, to international regulation, to international enforcement, the problem of eradicating money laundering via the Internet does not present itself with simple and easy solutions. However, as an international community, we must begin to take steps forward to reaching the common goal of crime prevention. We must all first agree that we have a serious problem on our hands, and that it therefore warrants serious consideration into solving it. The law often chases technology. Here the law must accept a challenge of technological complexity and international dimensions. Then we must proceed to the nuts and bolts of the dilemma and decide which are the tools that are needed to fix the situation at hand. Once we make it through this hoop, we must work together to enforcing our rules, and ensuring compliance with our laws. Only time will tell if we will be successful, but time is of the essence, and action must be taken.