Loyola of Los Angeles
Entertainment Law Review

Volume 16 | Number 3 Article 3

3-1-1996

Blackjack or Bust: Can U.S. Law Stop Internet Gambling

Seth Gorman

Anthony Loo

COMMENTS

BLACKJACK OR BUST: CAN U.S. LAW STOP INTERNET GAMBLING?

I. INTRODUCTION

Take a stroll down Money Lane. Three dimensional pictures with vivid colors illuminate your first stop on the Internet:[1] Casino Antigua. Next door is Casino Belize. Enter and meander through the virtual poker tables surrounded by virtual people and dealers. Virtual slot machines clang with awards, sounds blasting from the speakers attached to your personal computer. Across the way is the virtual lounge. Have a seat, have a virtual drink. Chat with the stars or have a live cyber-affair with a user from any part of the world. The technology is here and the program will soon follow.[2]

By September 1995, several Internet casinos opened their doors to accept wagers offshore.[3] By stationing offshore, these Internet casinos

---

1. The Internet is a huge web of about 30,000 interconnected computer networks, stretching across the globe. Established during the 1960s, it began as a military network, designed as a fail-safe system that could be fully activated in the event of war or public emergency. Phaedra Hise, *Net Profit,* INC., Oct. 1994, at 80. Later, the National Science Foundation set up the NSFnet, which ran lines to major universities and supercomputer centers, forming the backbone of the Internet. *Id.* As other governmental agencies and large corporate research departments plugged in, the interconnected network became known as the Internet. *Id.*

2. Joshua Quittner, *Betting on Virtual Vegas; To Get Around U.S. Gambling Laws, the First Online Casinos are Setting up Their Card Tables Offshore,* TIME, June 12, 1995, at 63. Virtual Vegas is perhaps the most active Internet casino. The casino entertainment center includes a Turbo Blackjack equipped with sassy dealers and artificial intelligence that the casino claims adapts to your game playing style as well as your savvy interactions. *See* http://www.virtualvegas.com/ (available as of Mar. 23, 1996). Not only does the entertainment center include games of chance, but also adds to the excitement by hosting a Ms. Metaverse beauty pageant, Amphitheater, a Lizard Lounge for personal chats with other users, and Megamall. *Id.*

3. *See generally* http://www.intersphere.com/bet/parlay.html (available as of Mar. 23, 1996); http://www.casino.org (available as of Mar. 23, 1996).

hope to avoid United States law enforcement, but still reap profits from American gamblers.[4]

Albeit neither in graphic three-dimensional form nor with vivid sounds, the popularity of these Internet casinos could be tremendous.[5] Although one site requires you first to send a cashier's check or moneygram to the casino,[6] another actually allows you to charge your wagers to your credit cards or withdraw money from your bank account through the use of an Internet currency.[7] You are then allowed to gamble or place bets on games of chance or sporting events. If you win, the casino will either mail your winnings to you or credit your account.[8]

Internet gambling has the potential of becoming a tremendous source of revenue. One estimate predicts that Internet gambling could produce as much as ten billion dollars in revenue from the United States alone.[9] First, capital outlays are minimal compared to the cost of constructing a live

---

4. Quittner, *supra* note 2, at 62. Warren Eugene, operator of Internet Casinos based in the Turks and Caicos Islands, exclaimed: "Money is beginning to pour in." Josh Romonek, *Entrepreneurs Open Casinos in Cyberspace Operators Say Their On-line Gambling Centers Will be Successful, but Bettors and Computer Enthusiasts Are Wary of Cheating by the House*, FORT WORTH STAR-TELEGRAM, Aug. 20, 1995, at 1. Eugene said he has registered nearly 8000 users, about 1000 of whom have set up gambling accounts in preparation for the September 1, 1995 opening. *Id.* "I'm at the door," he says, "I plan to make billions and billions upon billions of dollars." Quittner, *supra* note 2, at 64.

Another Internet gambling site, Global Casino, operated by Sports International Ltd. in Antigua, has allowed real-money betting over the Internet for a few months. Romonek, at 1. One feature that Global Casino currently offers is called "proposition wagers," which is a bet that is dependent on the outcome of a sporting event. The casino currently receives hundreds of calls daily about setting up accounts. *Id.*

5. William M. Bulkeley, *New On-line Casinos May Thwart U.S. Laws*, WALL ST. J., May 10, 1995, at B1.

6. Wagernet Casinos, http://www.vegas.com/wagernet (spot: 100) (on file with the *Loyola of Los Angeles Entertainment Law Journal*). Wagernet is a service of Global Gaming of Belize. This casino requires a $100 setup fee for necessary hardware and software. *Id.*

7. Virtual Vegas, http://www.virtualvegas.com/ (available as of Mar. 23, 1996); *see* discussion *infra* part IV.C. DigiCash is an electronic currency redeemable and exchangeable for various international hard currencies. *See* DigiCash, http://www.digi-Cash.com (available as of Mar. 23, 1996); *see also infra* part IV.C.

8. *See* Bulkeley, *supra* note 5, at B7.

9. *Chance a Flutter on the Internet; Hi-tech Firms Scent Big Profits as Betting and Blackjack Make Their Debuts on the Information Superhighway*, EVENING STANDARD, June 5, 1995, at 38. Ten billion dollars would constitute one fourth of the legal gambling revenue collected in the United States last year. *Id.* When foreign revenue is factored in with the $40 billion spent on legal gambling and the $30 billion spent on illegal gambling in the United States annually, Internet gambling reveals itself as a fast profit endeavor. *Computer Connection*, (CNN television broadcast, June 3, 1995) (transcript #9-1, at 1).

casino in the United States.[10] Second, the operating expense of an Internet casino is trivial compared to that of an actual casino.[11] Third, when operated in the Caribbean, the taxes are lower.[12]

As the Internet continues to gain exponentially in the number of users, living room gambling may proliferate to become a traditional weekend pastime.[13]

Although no case has so held, and the statutes that may regulate Internet gambling are not explicitly on point, the authors contend that Internet gambling is illegal under current laws. However, due to the difficulties in enforcement, the problems with jurisdiction, and the difficulties in applying antiquated laws to Internet gambling, law enforcement may not be able to enforce United States law on the offshore Internet casinos. For example, the existence of encryption technology, digital telephony, electronic money, tracing difficulties, personal jurisdiction, international comity and sovereignty may preclude the United States from enforcing its laws abroad.

The authors suggest that Internet gambling be conditionally legalized to avoid any jurisdictional, international comity and enforcement concerns. Under this approach, Internet gambling should be permitted only to casinos that block access to minors and submit to United States jurisdiction and its laws. Alternatively, Congress may prevent access to the Internet casinos by holding access providers liable if they permit any access to the casinos. Finally, Congress can promote family use of "blocking technology." Part II discusses the current gambling statutes and their weakness when applied to Internet casinos. Part III analyzes the jurisdictional and international comity concerns associated with applying United States criminal laws to casinos abroad. Part IV describes how technology will prevent current laws from being enforced. Part V proposes and analyzes solutions to effectively control or eliminate Internet gambling.

---

10. For example, Chicago wishes to bring in a large casino in the upcoming years. Starting costs are estimated at $2 billion dollars, and involves an expected 37,000 construction workers. CONG. REC. S10,912-04 (daily ed. July 31, 1995) (statement of Sen. Simon (D-Ill.)). By contrast, Internet Casinos needed only $10 million to start operations. Quittner, *supra* note 2, at 64.

11. Quittner, *supra* note 2, at 64.

12. Bulkeley, *supra* note 5.

13. Currently, an estimated 15 to 30 million people in 137 countries use the Internet. Mark L. Gordon & Diana J.P. McKenzie, *A Lawyer's Roadmap of the Information Superhighway*, 13 J. MARSHALL COMM. & INT'L L. J. 177, 182 (1995). Forrester Research, a technology resource firm, estimates that the commercial on-line computer-service market will become a $3 billion industry by 1998. This is up from the $530 million in revenue this year, as users branch out from chatting with other users to buying goods and services. Lourdes Lee Valeriano, *Business Bulletin*, WALL ST. J., Feb. 3, 1994, at A1.

II. APPLICABILITY OF UNITED STATES LAWS

This section analyzes the applicability of federal gambling statutes to offshore Internet casinos and the possible application of some of these statutes to access providers and players. Although this section does not discuss the application of federal laws to onshore casinos, the authors contend that Internet gambling is illegal regardless of whether the casinos are located onshore or offshore.[14]

Congress enacted the Federal Interstate Wire Act ("Wire Act"),[15] the Travel Act,[16] and the Organized Crime Control Act of 1970 ("Crime Control Act")[17] to prohibit gambling activities from crossing state lines and to combat gambling operations controlled and managed by organized crime.[18] Although these statutes may be effective in dealing with most types of gambling, questions remain as to the effectiveness of these statutes toward Internet gambling.[19]

---

14. For example, the Minnesota Attorney General recently filed suit against a virtual casino located in Las Vegas claiming that the casino violated state and federal laws. *Minnesota A.G. Files Legal Action Against Individuals Involved in Computer On-line Scams*, http://www.state.mn.us/ebranch/ag (posted July 18, 1995) (path: home> memo on jurisdiction) (on file with the *Loyola of Los Angeles Entertainment Law Journal*).

15. 18 U.S.C. § 1084 (1994).

16. *Id.* § 1952.

17. *Id.* § 1955.

18. H.R. REP. NO. 967, 87th Cong., 1st Sess. (1961), *reprinted in* 1961 U.S.C.C.A.N. 2631.

> The purpose of the bill is to assist the various States and the District of Columbia in the enforcement of their laws pertaining to gambling, bookmaking, and like offenses and to aid in the suppression of organized gambling activities by prohibiting the use of wire communication facilities which are or will be used for the transmission of bets or wagers and gambling information interstate and foreign commerce.

Id.

19. The analysis applied to these statutes and the gambling activities that they prohibit is also instructive of the analysis which would be applied to the RICO statutes. Due to the scope of this article and the complexity of the RICO statutes, an analysis will not be made under the RICO statutes. For discussions of the RICO statutes, see Susan W. Brenner, *RICO, CCE, and Other Complex Crimes: The Transformation of American Criminal Law?*, 2 WM. & MARY BILL RTS. J. 239 (1993); Pamela H. Bucy & Steven T. Marshall, *An Overview of RICO*, 51 ALA. LAW. 283 (1990); Thomas Fitzpatrick & Brian O'Neill, *Elements of a RICO Action, reprinted in* CRIM. LAW & URBAN PROB. 1990, at 7 (PLI Litig. & Admin. Prac. Course Handbook Series No. 155, 1990); Patrick A. Tuite & John L. Hines, Jr., *RICO's Pattern Requirement in the Seventh Circuit*, 5 CBA REC. 18 (Mar. 1991).

A. Section 1084: The Wire Act

One statute that applies to Internet gambling is the Wire Act.[20] The Wire Act provides, in pertinent part:

> Whoever being engaged in the *business of betting* . . . knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets . . . which entitles the recipient to receive money or credit as a result of bets . . . shall be fined under this title or imprisoned not more than two years, or both.[21]

This statute clearly applies to Internet casinos; however, it does not seem to apply to access providers and players.

1. Casinos

To find the Internet casinos guilty of violating the Wire Act, the government needs to prove the four elements of the Act. The government must establish: (1) the Internet casinos are in the business of betting; (2) the Internet casinos must know that the bets are being transmitted through a wire communication facility; (3) the bets must be transmitted in interstate or foreign commerce; and (4) the Internet casinos or the players must be able to receive money or credit as a result of the bets.[22]

First, the virtual casinos are clearly "engaged in the business of betting."[23] Courts have defined this term as any bookmaking operation that takes bets.[24] Internet casinos take bets from players on sporting events and casino games. Therefore, under this definition, Internet casinos should be considered to be engaged in the business of betting.

Second, the Internet casinos also knowingly use a wire communication facility to transmit bets. Gambling services are transmitted on the Internet which uses telephone lines to transmit information. This transmission violates the Wire Act because the Act prohibits gambling businesses from using the telephone or telex for interstate gambling.[25]

Third, the Internet casinos transmit bets in interstate or foreign commerce using the Internet. The Internet is a global network that crosses

---

20. 18 U.S.C. § 1084 (1994).
21. *Id.* § 1084(a) (emphasis added).
22. *Id.*
23. United States v. Baborian, 528 F. Supp. 324, 328 (D.R.I. 1981).
24. *Id.*
25. I. Nelson Rose, *Gambling and the Law*, REPLAY MAG., July 1995, at 46.

the borders of many states and countries. Thus, when a player in California places a bet with an Internet casino in the Caribbean, the bet is transmitted in foreign commerce.

Finally, Internet casinos or players receive money or credit that results from the bets. Players place their wagers with Internet casinos and depending on whether the players win or lose, either the casinos or the players will be the recipients of the bets.

Furthermore, not only does the Wire Act prohibit placing bets, but it also prohibits the transmission of "information assisting in the placing of bets."[26] Thus, even a casino that does not actually take wagers from players can violate the Wire Act.

For instance, a virtual casino called Wagernet does not actually take bets from players, but matches players who bet on sporting events.[27] Wagernet will place a player's proposition on the network for others to accept.[28] In return, it will take a transactional fee of two-and-a-half percent.[29] The casino may argue that it does not engage in the "business of betting" because it does not take wagers from players but merely matches players together. However, players who are matched with other players would still receive money or credit as a result of the bet. Law enforcement authorities will likely prevail in arguing that casinos like Wagernet are still violating the Wire Act because they provide the necessary medium for players, who would otherwise have no access to other players to match up with.

2. Access Providers

The government may try to prohibit Internet casinos from offering their games to players in the United States by prosecuting the "access providers" under § 1084(d) of the Wire Act.[30] However, the clear language of the statute restricts the government from doing so. Section 1084(d) provides, in pertinent part:

> When any common carrier, subject to the jurisdiction of the Federal Communications Commission, is notified in writing by a Federal, State, or local law enforcement agency, acting within its jurisdiction, that any facility furnished by it is being used or will be used for the purpose of transmitting or receiving

---

26. 18 U.S.C. § 1084(a).
27. Bulkeley, *supra* note 5.
28. *Id.*
29. *Id.*
30. 18 U.S.C. § 1084(d).

> gambling information in interstate or foreign commerce in violation of Federal, State or local law, it shall discontinue or refuse, the leasing, furnishing, or maintaining of such facility.[31]

Section 1084(d) of the Wire Act appears to allow law enforcement authorities to notify the access provider that its customers are using its facility for the purpose of transmitting or receiving gambling information in interstate or foreign commerce. However, for law enforcement to mandate the providers to discontinue providing such services, the providers must be subject to the jurisdiction of the Federal Communication Commission ("FCC").[32] At this time, Congress has not explicitly subjected the Internet or its providers to the jurisdiction of the FCC. Thus, unless Congress requires the providers to be licensed by the FCC, § 1084(d) of the Wire Act does not apply to access providers.

3. Players

If authorities are unable to curb Internet gambling by prosecuting either the casinos or the access providers, then they may look to the players as a possible means of regulating Internet gambling. However, the congressional intent of the Wire Act was not to prosecute players.[33] The legislative history of the Act contains the following observation: "[l]aw enforcement is not interested in the casual dissemination of information . . . between acquaintances. That is not the purpose of this legislation."[34] Rather, the intent of Congress was that the Wire Act apply to gambling businesses and not to mere players.[35]

In *United States v. Baborian*, a mere player was prosecuted under the Wire Act.[36] The defendant in *Baborian* was a player who wagered an average of $800 to $1000 a day, three to four times a week.[37] The court held that regardless of the fact that wagers were substantial and the player displayed the sophistication of an expert in odds making, the statute did not apply to him because Congress did not contemplate prohibiting the activities of mere players.[38]

---

31. *Id.*
32. Bulkeley, *supra* note 5.
33. S. REP. No. 588, 87th Cong., 1st Sess. 3 (1961).
34. *Id.*
35. United States v. Baborian, 528 F. Supp. 324, 328 (D.R.I. 1981).
36. *Id.* at 324.
37. *Id.* at 326.
38. *Id.* at 328-29.

The statute may apply to players only if they perform a integral function of the gambling business,[39] such as being an agent or an employee of the gambling operation, sharing in the profits or losses of the business, or receiving compensation for their participation.[40] The facts in *Baborian* do not indicate that the defendant was an agent or an employee of the gambling operation.[41]

B. Section 1952: The Travel Act

Another federal gambling statute that may be applicable to Internet gambling is the Travel Act.[42] This Act seems applicable to both Internet casinos and its players. The Travel Act provides, in relevant part:

> (a) Whoever travels in interstate or foreign commerce . . . with intent to—(1) distribute the proceeds of any unlawful activity . . . (3)(B) shall be fined [or] . . . imprisoned for not more than twenty years, or both. . . . (b) As used in this section (i) "unlawful activity" means (1) any business enterprise involving gambling.[43]

The Travel Act prohibits anyone from traveling or using any facility in interstate or foreign commerce with the intent to promote or carry on any unlawful activity.[44] Unlawful activity includes "any business enterprise involving gambling . . . in violation of the laws of the State in which they are committed or of the United States."[45]

Furthermore, cases have held that the scope of the unlawful activity includes the transportation of gambling activities via telephone lines. In *United States v. Smith*,[46] the defendant claimed that the Travel Act applied only to transportation facilities and not to the use of a telephone facility.[47] However, the Illinois District Court held that "facilities," as used in the Travel Act, means *interstate* facilities of every kind and is not limited to just the actual physical transportation of substantive material into interstate

---

39. *Id.* at 329.
40. *Baborian*, 528 F. Supp. at 329.
41. *Id.* at 328-29.
42. 18 U.S.C. § 1952 (1994).
43. *Id.*
44. *Id.* The purpose of the Travel Act is to permit the federal government to act against members of organized crime and to provide federal assistance to local law enforcement against criminal activities extending beyond borders of the state. United States v. Lightfoot, 506 F.2d 238, 240-41 (D.C. Cir. 1974).
45. 18 U.S.C. § 1952(b)(1).
46. 209 F. Supp. 907 (E.D. Ill. 1962).
47. *Id.* at 915.

commerce.[48] To otherwise limit the scope of this statute defeats its purpose of precluding the use of interstate commerce for illegal gambling.[49] The court noted that the Travel Act can be used to regulate interstate gambling because telephone voices are "actually transported by wires across state lines to the same extent as materials are transported over state lines in moving vehicles."[50]

Thus, the transportation of gambling activities across state lines via the Internet violates the Travel Act. Although the analysis under the Travel Act is similar to that under the Wire Act, the Travel Act is broader because it does not require the proscribed activity to be a gambling business.[51] The Travel Act applies not only to Internet casinos, but it also seems to apply to players who use interstate facilities for the transportation of unlawful activities.

C. Section 1955: The Crime Control Act

The Crime Control Act seems applicable only to Internet casinos because the Act only prohibits gambling businesses involving five or more persons.[52] Congress intended that this section combat large scale illegal gambling activities.[53] It does not seem applicable to players or to access providers because they are not considered gambling businesses.

Under § 1955, it is a federal crime for a gambling business to violate state law.[54] The Act provides, in pertinent part:

> (a) Whoever conducts . . . an illegal gambling business shall be fined under this title or imprisoned not more than five years, or both. (b) As used in this section—(1) "illegal gambling business" means a gambling business which—(i) is a violation of the law of a *State* . . . in which it is conducted; (ii) involves five or more persons who *conduct* . . . all or part of such business; and (iii) 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.[55]

---

48. *Id.* at 916.
49. *Id.*
50. *Id.*
51. *See* 18 U.S.C. § 1952.
52. *Id.* § 1955.
53. *See* I. NELSON ROSE, GAMBLING & THE LAW 49 (1986).
54. 18 U.S.C. § 1955 (1994).
55. *Id.* (emphasis added).

The statute does not require that the casino operators be found guilty in state court.[56] Rather, the statute requires only that there be a state law,[57] the gambling business involves five or more persons,[58] remains in substantially continuous operation for more than thirty days, and violates some state law, no matter how trivial.[59]

In analyzing § 1955, the Supreme Court defined "conduct" as "any degree of *participation* in an illegal gambling business, except participation as a mere bettor."[60] However, the term "participation" is limited to the performance of acts that are necessary or helpful to the gambling business.[61]

The necessary proof that the government must proffer in a § 1955 violation is minimal. "The government need not prove that the same five persons participated for thirty days."[62] Nor does the government have to prove that the five persons were active every day.[63] All that the government needs to prove is that at least five persons, at all times during a thirty day period, conducted the illegal gambling activity.[64] It is likely that a virtual casino could require at least five individuals for its operation. As long as they are considered necessary and helpful, they fulfill the requirement.[65] Thus, computer operators, computer maintenance crews, accountants, and owners may all be included even though their participation may not relate to the actual gambling.

The courts have also been rather liberal in applying the statutory requirement of thirty continuous days of operation. Some circuits have held that if the government can establish a repeated pattern of gambling activity, even if surveillance was not conducted for a continuous thirty day period, the jury can infer that the gambling operation took place continuously for that period.[66] Accordingly, even if an Internet casino

---

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

57. 18 U.S.C. § 1955(b)(i).

58. *Id.* § 1955(b)(1)(ii).

59. *Id.* § 1955(b)(1)(iii).

60. Sanabria v. United States, 437 U.S. 54, 70-71 n.26 (1978) (emphasis added).

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

62. United States v. Murray, 928 F.2d 1242, 1246 (1st Cir. 1991).

63. *Id.*

64. *Id.*

65. *DiMuro*, 540 F.2d at 508.

66. United States v. Allen, 588 F.2d 1100, 1104 (5th Cir. 1979), *cert. denied*, 441 U.S. 965 (1979) (the jury could infer that the gambling activity occurred continuously for 30 day periods by a showing of a repeated pattern of gambling activity established over a period of several months); United States v. Nerome, 563 F.2d 836, 843 (7th Cir. 1977), *cert. denied*, 435 U.S. 951 (1978) (evidence of gambling activity occurring almost two days every weekend for eight months

operated on a sporadic basis, the argument that it failed to satisfy the statutory requirement of substantial continuous operation for a period in excess of thirty days would most likely fail.

D. Aiding and Abetting Under The Crime Control Act

An access provider may be charged with violating the Crime Control Act under the theory of accomplice liability.[67] However, some courts are reluctant to apply such liability because "[t]he penalties for violating § 1955 are much more severe than the penalties for violating the predicate state law crimes."[68] For instance, an unlawful gambling activity may only be a misdemeanor crime under state law, but under § 1955, this misdemeanor becomes a federal crime subject to large fines and felony imprisonment.[69] To subject access providers to the penalties of § 1955 seems rather harsh since the providers are only providing access to those who wish to use the Internet. The effect of such a severe penalty would possibly cause the providers either to police every transmission that comes through their services or to restrict access for fear of being prosecuted.

Congress passed these gambling statutes and severe penalties to combat organized crime and significant gambling operations.[70] Charging access providers with "aiding and abetting" may thwart this congressional intent because the only role of the providers is to furnish access to the Internet. This role is neither in violation of any criminal statute nor comparable to the activity of organized crime.

On the other hand, if an access provider assisted an Internet casino in more ways than just granting access, then this provider may be considered an aider and abettor. However, the amount of assistance necessary to become an aider and abettor of illegal gambling should depend on the requisite level of mens rea.[71]

---

was sufficient for the jury to infer that the gambling took place on more than thirty individual days).

67. 18 U.S.C. § 2 (1995). "Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal." *Id.*

68. United States v. Hill, 55 F.3d 1197, 1202 (6th Cir. 1995). The maximum penalty under § 1955 is $20,000 and a five year prison term. *Id.*

69. *Id.* at 1199.

70. H.R. REP. NO. 967, 87th Cong., 1st Sess. (1961), *reprinted in* 1961 U.S.C.C.A.N. 2631.

71. *Compare* United States v. Leon, 534 F.2d 667, 674-75 (6th Cir. 1976) (the defendant's lack of knowledge that the gambling operation involved more than five persons did not change the harm imposed on society) *with Hill*, 55 F.3d at 1202 ("The aider and abettor must assist the principal with the intent of making the illegal gambling business succeed.").

Some circuits have held that a defendant accused of a substantive violation of § 1955 need not have knowledge of all the components of the statute, such as the five persons requirement.[72] For instance, in *United States v. Smaldone*,[73] the Tenth Circuit held that a defendant takes the risk of violating federal law when he violates a state gambling statute because § 1955 is not a specific intent statute.[74] The defendants were convicted of a federal crime even though their illegal gambling activities only violated misdemeanor state statutes.[75] Thus, under this analysis, an access provider, just by granting access, would be held liable as an aider and abettor because the government would not have to prove that the providers knowingly assisted in the gambling activity.

On the other hand, in *United States v. Hill*,[76] the Sixth Circuit held that one aids and abets a gambling operation when one has "knowledge of the general scope and nature of the illegal gambling business."[77] The aider and abettor must also take action that demonstrates the "intent of making the illegal gambling business succeed."[78] This bright-line rule seems to be the more persuasive standard in holding an access provider to be an aider and abettor. Under this standard, the mere transmission of the gambling activity would be insufficient to hold the access provider liable. The access provider would have to provide certain assistance, such as collection of bets, to be considered an aider and abettor.

Because the Interstate Wire Act, the Travel Act, and the Crime Control Act encompass the transportation of wagering information over the telephone wires, they are applicable to Internet gambling.[79] First, casinos that offer Internet gambling are in violation of the Wire Act because they are gambling businesses that knowingly use telephone wires to transmit bets in foreign commerce, which entitles them to receive money or credit

---

72. *See* United States v. Cyprian, 23 F.3d 1189, 1199 (7th Cir.), *cert. denied*, 115 S. Ct. 211 (1994) (though defendant did not know gambling activity was illegal, requisite state of mind is not expressly required by the statute); United States v. Leon, 534 F.2d 667, 675 (6th Cir. 1976).

73. 485 F.2d 1333 (10th Cir. 1973), *cert. denied*, 416 U.S. 936 (1974).

74. *Id.* at 1348-49.

75. *Id.* at 1343-44. Although the three statutes were repealed prior to the commencement of the case, the Colorado Revised Statute required all offenses committed prior to the effective date of the revised codes to be "tried and disposed of according to the provisions of law existing at the time of the commission . . . ." *Id.* at 1344 n.6 (quoting COLO. REV. STAT. § 40-1-103(2) (1972)).

76. 55 F.3d 1197 (6th Cir. 1995).

77. *Id.* at 1201.

78. *Id.* at 1202.

79. The three statutes seem to apply only to gambling businesses or players, but they do not seem to apply to access providers.

as a result of the bets. Second, Internet casinos and players are violating the Travel Act if they intend the unlawful gambling activity to be transmitted in interstate or foreign commerce. Finally, Internet casinos are in violation of the Crimes Control Act if their gambling activities violate state law. Law enforcement would need only to establish that the operation involved five or more persons and was ongoing for a period of thirty days.

However, the global nature of the Internet makes enforcement of these statutes difficult. Thus, the two key issues when dealing with Internet gambling, especially when the accused resides abroad, are whether United States courts have personal jurisdiction over prospective defendants, and whether such jurisdiction can be enforced.

III. JURISDICTION AND INTERNATIONAL COMITY

The United States' power to exercise personal jurisdiction over Internet casinos poses challenging questions on the limits of jurisdiction. Part III analyzes the jurisdictional quagmire the Internet presents in criminal prosecutions and proposes models for jurisdiction. Part III.B. discusses sovereignty and international comity concerns.

A. The Jurisdictional Quagmire and Models for Jurisdiction

Applying *International Shoe Co. v. Washington*[80] to Internet casinos poses the question whether the casino has had enough contacts with the state in which the federal court is located to make the exercise of jurisdiction fair.[81]

A two-part inquiry into minimum contacts and fairness insures a proper substitute for physical presence[82] and gives defendants "fair warning that a particular activity may subject [them] to the jurisdiction of a foreign sovereign."[83]

---

80. 326 U.S. 310 (1945).

81. *Id.* at 316. According to the Court:

> "[D]ue process requires only that in order to subject a defendant to a judgment *in personam*, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"

Id. (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)).

82. Burnham v. Superior Ct., 495 U.S. 604, 618 (1990); Shaffer v. Heitner, 433 U.S. 186, 203 (1977); *see also* Pennoyer v. Neff, 95 U.S. 714, 733 (1877).

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

First, minimum contacts for specific jurisdiction[84] may be achieved when the defendant has "purposefully directed" activities at the forum state.[85] Such contact must not be accidental or attenuated,[86] but rather a "substantial connection"[87] where the corporation or individual "manifestly has availed himself of the privilege of conducting business there."[88]

Second, "traditional notions of fair play and substantial justice" require that the exercise of jurisdiction be reasonable.[89] Often this inquiry is phrased in terms of the foreseeability of being brought into the jurisdiction: is the "defendant's conduct and connection with the forum State . . . such that he should reasonably anticipate being haled into court there?"[90] Or phrased another way, has the defendant had enough contact with the state so as to render it "unfair to allow . . . [the defendant] to escape having to account in other States for consequences that arise proximately from such activities"[91] and the laws of that state. And, of course, the alleged injury must proximately relate to these contacts.[92]

1. Minimum Contacts, Foreseeability, and Purposeful Availment

To avoid jurisdiction, operators of Internet casinos will argue that there are insufficient contacts. They will argue that the requisite minimum contacts do not exist merely because a consumer brings a product, such as

---

84. The Supreme Court described the difference between specific and general jurisdiction. "It has been said that when a State exercises personal jurisdiction over a defendant in a suit arising out of or related to the defendant's contact with the forum, the State is exercising 'specific jurisdiction' over the defendant." Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414 n.8 (1984). "When a State exercises personal jurisdiction over a defendant in a suit not arising out of or related to the defendant's contacts with the forum, the State has been said to be exercising 'general jurisdiction' over the defendant." *Id.* at 414 n.9.

85. *Burger King*, 471 U.S. at 472; Calder v. Jones, 465 U.S. 783 (1984); Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 774 (1984).

86. *Keeton*, 465 U.S. at 774.

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

88. *Burger King*, 471 U.S. at 476.

89. International Shoe v. Washington, 326 U.S 310, 320 (1945).

90. *World-Wide Volkswagen*, 444 U.S. at 297.

91. *Burger King*, 471 U.S. at 474. Justice Brennan captured this point effectively in stating:

> [W]here individuals "purposefully derive benefit" from their interstate activities, it may well be unfair to allow them to escape having to account in other States for consequences that arise proximately from such activities; the Due Process Clause may not readily be wielded as a territorial shield to avoid interstate obligations that have been voluntarily assumed.

Id. at 473 (citation omitted).

92. Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414 (1984).

a car, into the state.[93] Similarly, according to the Court, "the placement of a product into the stream of commerce, without more, is not an act of the defendant purposefully directed toward the forum State."[94] Some examples of sufficient contacts may include "designing the product for the market in the forum State, advertising in the forum State, establishing channels for providing regular advice to customers in the forum State, or marketing the product through a distributor who has agreed to serve as the sales agent in the forum State."[95]

Internet casino operators may argue that although it was foreseeable that some United States residents may access their services, the casinos have not directed their activities at the United States. Casino operators have not advertised gambling in the United States, nor hired a distributor or agent to promote the service directly. Neither is the product designed exclusively for the United States.

Furthermore, it may be argued that merely placing a product, an interactive gambling casino, in the stream of commerce does not equate to "purposeful direction" or "availment" of United States jurisdiction. Nor does making it possible or convenient for the product to be brought into the jurisdiction, by virtue of placing this gambling on the Internet, subject the casino operator to the United States jurisdiction.

However, law enforcement will counter that far from being sporadic, accidental, or attenuated, the connection of the Internet casino to the United States may be considered substantial. For instance, in a standard blackjack hand, the foreign casino sends dozens of images to the United States. There is an interaction, a back-and-forth communication, in which each side responds and reacts to the other. This interaction may demonstrate a "substantial connection."

Further, law enforcement will argue that providing Internet gambling is purposeful. The casino operator clearly intends these contacts: like a bullet, the casino's signals are shot to hit its target, the customer.[96] The casino signals are purposefully sent to reach clients and carry on interactive conversations through the Internet with the expectation that the foreign clients will respond. Thus, the activity and contact with the United States

---

93. *World-Wide Volkswagen*, 444 U.S. at 295.

94. Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102, 112 (1987).

95. *Id.*

96. State v. Rossbach, 288 N.W.2d 714 (Minn. 1980). In this case, the defendant was standing inside the borders of an Indian Reservation when he fired a rifle across the boundary line at a person outside the border. *Id.* Although the defendant claimed that Minnesota courts lacked jurisdiction because his act took place outside of Minnesota, the Minnesota Supreme Court held that intentional impact within Minnesota land created jurisdiction. *Id.* at 715.

appear intentional and purposeful, availing the casino operator of United States jurisdiction.

2. Comparability to Telephone Services

One may argue that casino services are on par with a telephone service accessible from around the world. Courts have held that telephone calls and information transmitted through these calls, standing alone, are not sufficient to confer personal jurisdiction.[97] For instance, courts have held that a "telephone service which allows people to call the bank from all parts of the country and world to perform banking transactions . . . does not commit the bank to national jurisdiction."[98] Similarly, use of an out-of-state online database through a local telephone service,[99] use of a credit card from an out-of-state corporation,[100] or a transaction of business through an 800 toll-free number[101] does not commit one to the courts of that foreign jurisdiction.

3. Analogies to Telephone Auctions and Business Transactions

Conversely, law enforcement may argue that Internet gambling is analogous to *Parke-Bernet Galleries, Inc. v. Franklyn*.[102] In this case, the defendant participated in an auction via telephone.[103] This conduct essentially placed the defendant in the auction room as a bidder for the auctioned items. The court held that although the defendant was not physically present in the forum state, his conduct was sufficient to exercise personal jurisdiction.[104]

Law enforcement will also argue that the acts of an Internet gambling casino are analogous to a businessperson's telephone transactions, which

97. T.J. Raney & Sons, Inc. v. Security Savings & Loan Assoc., 749 F.2d 523 (8th Cir. 1984) ("The use of interstate mail, telephone or banking facilities, standing alone, was insufficient to satisfy the requirements of due process.") *Id.* at 525.

98. Resolution Trust Corp. v. First of America Bank, 796 F. Supp. 1333, 1336 (C.D. Cal. 1992).

99. Pres-Kap, Inc. v. System One, Direct Access, Inc., 636 So. 2d 1351, 1353 (Fla. Dist. Ct. App. 1994); Michael J. Santisi, Pres-Kap, Inc. v. System One, *Direct Access, Inc: Extending the Reach of the Long-Arm Statute Through the Internet?*, 13 J. MARSHALL COMP. & INFO. L. 433, 441 (1995).

100. First Nat'l Monetary Corp. v. Chesney, 514 F. Supp. 649, 653 (E.D. Mich. 1980).

101. Standard Enter., Inc. v. Bag-It, Inc., 673 F. Supp. 1216, 1220 (S.D.N.Y. 1987).

102. 256 N.E.2d 506 (N.Y. App. Div. 1970).

103. *Id.* at 507.

104. *Id.* at 509.

are sufficient to establish personal jurisdiction.[105] As if it were a businessperson, the casino responds and reacts to proposals transmitted over the telephones. The cases relating to telephone transactions firmly establish that jurisdiction cannot be skirted by conducting an illegal activity in a foreign jurisdiction when the foreign participant is virtually present within the forum state.[106]

4. Similarities to Direct Mail Order or Publishing

Law enforcement will also argue that casinos resemble a direct mail order or publishing house. Casino operators send material around the world, thus impacting many locations. The federal courts in the states where casinos cause this harm should be able to bring wrongdoers to justice. In *Keeton v. Hustler Magazine*,[107] the wrongdoer published a libelous article in an out-of-state magazine.[108] The Court held that:

> Respondent's activities in the forum may not be so substantial as to support jurisdiction over a cause of action unrelated to those activities. But respondent is carrying on a "part of its general business" in New Hampshire, and that is sufficient to support jurisdiction when the cause of action arises out of the very activity being conducted, in part, in New Hampshire.[109]

Similarly, in *Calder v. Jones*,[110] the Court held that the exercise of jurisdiction by California over an out-of-state defendant was sufficient to satisfy the standards of due process.[111] According to the Court, California was the "focal point" of both the story and the harm suffered, making it sufficient to establish jurisdiction.[112]

---

105. PaineWebber Inc. v. Westgate Group, Inc., 748 F. Supp. 115, 121 (S.D.N.Y. 1990) (frequent telephone calls and telecopies are insufficient to establish personal jurisdiction in this case); China Union Lines v. American Marine Underwriters, 454 F. Supp. 198, 202 (S.D.N.Y. 1978) (letters, telephone calls and telex messages sufficient for jurisdiction); Otterbourg, Steindler, Houston & Rosen P.C. v. Shreve City Apartments, 543 N.Y.S.2d 978 (App. Div. 1989) (use of an open telephone line to respond to proposals sufficient for jurisdiction).

106. *See* sources cited *supra* note 105.

107. 465 U.S. 770 (1984).

108. *Id.*

109. *Id.* at 779-80.

110. 465 U.S. 783 (1984).

111. *Id.* at 788.

112. *Id.* at 789.

5. Similarities to Mass Torts and the Common Economic Pond

Alternatively, law enforcement may argue that jurisdiction for criminal actions on the Internet should model mass tort litigation. The connection between mass torts and the Internet may at first glance seem more attenuated than that between apples and oranges. However, they are similar because both transcend territorial borders and both defeat logical application of traditional tests of personal jurisdiction.

In mass tort cases, the traditional personal jurisdiction test often produced unjust results.[113] For some time, the judiciary has pondered the concept of a "common economic pond" or "national economic network."[114] The innovation of the common economic pond or national market ameliorates this injustice, allowing an individual to sue the producer of a product in the place of injury, without the need to analyze minimum contacts and purposeful availment.

The common economic pond was best described in the recent *In re DES Cases*.[115] The district court found personal jurisdiction over all the manufacturers regardless of their individual contacts with a particular state because all dropped their product into the common economic pond or national market.[116] The court ruled that to establish a prima facie case for the exercise of personal jurisdiction, the mere existence of an "appreciable state interest" is sufficient.[117] However, the defendant may

---

113. *See* Patrick J. Borchers, *Jurisdictional Pragmatism: International Shoe's Half-Buried Legacy*, 28 U.C. DAVIS L. REV. 561, 585 (1995).

114. *See In re* DES Cases, 789 F. Supp. 548, 576 (E.D.N.Y. 1992), *appeal dismissed*, 7 F.3d 20 (2d Cir. 1993). Some notable expositions of the concept include Justice Brennan's concurring opinion in *Asahi Metal Indus. v. Superior Court* ("[t]he stream of commerce refers not to unpredictable currents or eddies, but to the regular and anticipated flow of products from manufacture to distribution to retail sale,") and Justice Marshall's dissent in *World-Wide Volkswagen*, 444 U.S. at 314 ("[J]urisdiction is premised on the deliberate and purposeful actions of the defendants themselves in choosing to become part of a nationwide, indeed a global, network for marketing and servicing automobiles.").

115. *In re* DES Cases, 789 F. Supp. 552 (E.D.N.Y. 1992). *In re DES* was a complex civil action involving many suits against the developers of a synthetic estrogen designed to prevent miscarriages. *Id.* Unfortunately, many children were born deformed. *Id.* at 558. For a good discussion of the mass torts litigation and the challenges to personal jurisdiction, see Julia Christine Bunting, Ashley v. Abbott Laboratories: *Reconfiguring the Personal Jurisdiction Analysis in Mass Tort Litigation*, 47 VAND. L. REV. 189, 214 (1994).

116. *In re DES Cases*, 789 F. Supp. at 589.

117. *Id.* at 587.

defeat jurisdiction by arguing undue hardship.[118]

The Internet is similar to such a common economic pond because producers from around the world drop their goods and services into the Internet. As a result, jurisdiction is acquired at any point the Internet touches, as long as the country and state have an "appreciable interest" in the litigation (such as injury to a resident)[119] and the burden of defending the suit in that state is not unreasonable.

B. International Comity and Sovereignty

Extraterritorial application of federal legislation is a vague and uncontoured realm, that has some international and judicial guidance but remains unclear.[120]

---

118. *In re DES Cases* set forth a two-part test that can be applied to Internet transactions:

> I. The court must first determine if the forum state has an appreciable interest in the litigation, i.e., whether the litigation raises issues whose resolution would be affected by, or have a probable impact on the vindication of, policies expressed in the substantive, procedural or remedial laws of the forum. If there is an appreciable state interest, the assertion of jurisdiction is *prima facie* constitutional.
>
> II. Once a *prima facie* case is made, the assertion of jurisdiction will be considered constitutional unless, given the actual circumstances of the case, the defendant is unable to mount a defense in the forum state without suffering relatively substantial hardship.
>
> Evidence to be considered in determining the defendant's relative hardship includes, *inter alia*, (1) the defendant's available assets; (2) whether the defendant has or is engaged in substantial interstate commerce; (3) whether the defendant is being represented by an indemnitor or is sharing the cost of the defense with an indemnitor or co-defendant; (4) the comparative hardship defendant will incur in defending the suit in another forum; and (5) the comparative hardship to the plaintiff if the case were dismissed or transferred for lack of jurisdiction.

Id.

119. *Id.*; *see* Patrick J. Borchers, *Comparing Personal Jurisdiction in the United States and the European Community: Lessons for American Reform*, 40 AM. J. COMP. L. 121, 145 (1992). The European Community established that jurisdiction shall exist in the place of injury. *In re DES Cases*, 789 F. Supp. at 587.

120. *See generally* Ethan A. Nadelmann, *The Role of the United States in the International Enforcement of Criminal Law*, 31 HARV. INT'L L.J. 37 (1990). Professor Nadelmann compares the United States to the European countries in their international law enforcement relations. *Id.* He postulates that the United States has only recently had to adapt its law enforcement policies to a global scale, whereas Europe has had a history of international law enforcement cooperation. *Id.* at 37-38.

1. United States Laws Can Be Applied Abroad

It is clear that Congress has the power to pass legislation that regulates extraterritorial conduct.[121] In fact, United States courts have enforced the nation's laws outside of the territorial United States from as early as 1818.[122]

However, not all laws apply outside of the borders of the United States. The first step in determining whether United States laws apply extraterritorially is to look at the express language of the law and the congressional intent.[123] The next is to determine whether enforcement or application of United States law conflicts with protection afforded internationally. For instance, enforcement of a subpoena of bank records may conflict when the bank exists in another country and that country's laws protect bank records from subpoena.

---

121. EEOC v. Arabian Am. Oil, 499 U.S. 244, 246 (1991). "Both parties concede, as they must, that Congress has the authority to enforce its laws beyond the territorial boundaries of the United States." *Id.*

122. United States v. Palmer, 16 U.S. (3 Wheat.) 610, 630 (1818) (involving the power of defining and punishing piracy, even though they may be foreigners); *see* Gary B. Born, *A Reappraisal of the Extraterritorial Reach of United States Law*, 24 LAW & POL'Y INT'L BUS. 1, 14 (Fall 1992). Born notes: "[T]here is no real reason to doubt the soundness of these decisions, notwithstanding some arguably inconsistent language in early cases." *Id.* In broad language, these early cases swept aside prohibitions against extraterritorial enforcement of state laws. These cases arose when the regulations of one state came in conflict with those of another or with an Indian reservation. *Id.* at 13-14. *See, e.g.*, Rose v. Himely, 8 U.S. (4 Cranch) 241, 279 (1808) ("Legislation of every country is territorial; that beyond its own territory, it can only affect its own subjects or citizens.").

Also, the United States may enforce its laws even in opposition to those international treaties to which it is a signatory. United States v. Dion, 476 U.S. 734, 738 (1986). But the Constitution states that both these international treaties and those laws passed by Congress are the supreme law of the land. U.S. CONST. art. VI, § 2; *see also* Whitney v. Robertson, 124 U.S. 190, 194-95 (1887).

123. *See* FTC v. Compagnie De Saint-Gobain-Pont-a-Mousson, 636 F.2d 1300, 1306-07 (D.C. Cir. 1980) (concerning the FTC's use of registered mail to serve a subpoena duces tecum on a company in France; on the company's refusal, the appellate court found that Congress had not specifically granted the power to undertake such service). *Id.* Gary E. Davidson, *Congressional Extraterritorial Investigative Powers: Real or Illusory?*, 8 EMORY INT'L L. REV. 99, 118 (1994). (Laws are presumed to apply only within the territorial jurisdiction of the United States.) *Arabian Am. Oil*, 499 U.S. 244 (1991). "It is a longstanding principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." *Id.* at 248 (quoting Foley Bros., Inc. v. Filardo, 336 U.S. 281 (1949)).

2. Courts Should Exercise Discretion and Apply a Balancing Test to Protect International Comity

When a conflict exists for collecting evidence abroad, courts have great discretion in deciding whether to enforce United States' laws internationally.[124] The American Law Institute's *Third Restatement of the Foreign Relations Law of the United States* recommends that when a conflict arises, courts should perform a balancing analysis of the many concerns involved.[125] This balancing rests on the foundation of the principles of comity and sovereignty[126] so that courts reasonably limit their exercise of jurisdiction.[127]

---

124. Societe Nationale Industrielle Aerospatiale v. United States Dist. Court, 482 U.S. 522, 539-40 (1987). In dealing with discovery, punishable by French law but discoverable pursuant to the Federal Rules of Civil Procedure, a five justice majority concluded that lower courts should apply an international comity analysis on a case-by-case basis to determine the applicability of the Hague Convention. *Id.* at 544.

125. Section 403 of the Third Restatement provides several factors that courts should consider in deciding jurisdictional conflicts:

> (a) the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory;
> (b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect;
> (c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted;
> (d) the existence of justified expectations that might be protected or hurt by the regulation;
> (e) the importance of the regulation to the international political, legal, or economic system;
> (f) the extent to which the regulation is consistent with the traditions of the international system;
> (g) the extent to which another state may have an interest in regulating the activity; and
> (h) the likelihood of conflict with regulation by another state.

RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403 (1987).

126. A definition of "sovereignty" was articulated by Chief Justice Marshall in *Schooner Exchange v. M'Faddon*, 11 U.S. (1 Cranch) 116 (1812). "The jurisdiction of the nation within its own territory is necessarily exclusive and absolute. It is susceptible of no limitation not imposed by itself. Any restriction upon it, deriving validity from an external source, would imply a diminution of its sovereignty to the extent of the restriction . . . ." *Id.* at 135. More than eighty years later, the court defined "comity" as "the 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, and to the rights of its own citizens or of other persons who are under the protection of its laws." Hilton v. Guyot, 159 U.S. 113, 163-64 (1895).

127. Banco Nacional de Cuba v. Sabbatino, 376 U.S. 398, 428-32 (1964).

However, courts have traditionally abstained from hearing those cases which will call into question the wisdom or validity of a foreign sovereign's laws or protections.[128] Chief Justice Fuller stated the principle clearly in *Underhill v. Hernandez*:[129]

> Every sovereign State is bound to respect the independence of every other sovereign State, and the courts of one country will not sit in judgment on the acts of the government of another done within its own territory. Redress of grievances by reason of such acts must be obtained through the means open to be availed of by sovereign powers as between themselves.[130]

These principles further the United States' interest in stabilizing its international legal and commercial relations[131] and the separation of powers between the judicial and executive branches in the realm of foreign relations.

3. Separation of Powers

What the judicial branch deems crucial for mutual respect for each sovereign's laws and what is in the best interest of the nation in establishing a rule of comity among nations may differ from the executive branch's viewpoint. In *Banco Nacional de Cuba v. L.F. Sabbatino*,[132] the Supreme Court was asked to invalidate Cuba's expropriation of the property of American businesses.[133] The Court declined to exercise jurisdiction over the matter, declaring that:

> However offensive to the public policy of this country and its constituent States an expropriation of this kind may be, we conclude that both the national interest and progress toward the goal of establishing the rule of law among nations are best served by maintaining intact the act of state doctrine in this realm of its application.[134]

After citing a long line of history and cases, beginning with a speech that John Marshall gave to the House of Representatives while still a

---

128. *See id.* at 398; Shapleigh v. Mier, 299 U.S. 468 (1937); Oetjen v. Central Leather Co., 246 U.S. 297 (1918).

129. 168 U.S. 250 (1897).

130. *Id.* at 252.

131. Born, *supra* note 122.

132. 376 U.S. 398 (1964).

133. *Id.*

134. *Id.* at 436-37; *see also* Ricaud v. American Metal Co., 246 U.S. 304 (1918) (expropriation of bullion in Mexico during the revolution).

representative,[135] the Court concluded that international comity is within the realm of foreign policy, over which the Executive Branch has primary authority.[136] According to the Court:

> [W]here the Executive Branch, charged as it is with the primary responsibility for the conduct of foreign affairs, expressly represents to the Court that application of the act of state doctrine would not advance the interests of American foreign policy, that doctrine should not be applied by the courts.[137]

In short, courts should follow the lead of the Executive Branch in foreign policy. If the President deems that enforcing a United States law abroad would not be in the interest of American foreign policy, the courts should not enforce it.

This becomes clearer in an example. Suppose a Caribbean nation, seeking tax revenue, grants official permission or allows an Internet casino to operate within its territory. If the President of the United States determines that prosecution of the casino is in the interests of the United States foreign policy, then the courts should follow the Executive Branch's lead. The courts should apply United States laws against the foreign Internet casinos. This means that the United States would not recognize that nation's laws on the matter and would directly interfere with the sovereignty of that nation.

Therefore, courts should independently balance the interests of the United States against the international destabilization that results from meddling with a foreign sovereign's act of state. Even when the Executive Branch expressly declares that exercising jurisdiction is in the interests of the United States, the courts may refrain from doing so. Deference to a foreign sovereign's act of state in some cases, is necessary to avoid the destabilization of international legal and commercial relations that results from exercising jurisdiction.

4. Enforcement of United States Laws Abroad Sacrifices International Comity

Deferring to the Executive Branch may be prudent in most cases. However, strengthening law enforcement abroad may lead to international

---

135. John Marshall stated, "the President is the sole organ of the nation in its external relations, and its sole representative with foreign nations." First Nat'l City Bank v. Banco Nacional de Cuba, 406 U.S. 759, 766 (1972).

136. *Id.* at 768.

137. *Id.*

destabilization of legal and commercial relations. Some destabilization has already occurred.[138] Since the 1970s, legislation has been enacted to increase the United States' presence abroad.[139] This increase is an attempt to fight crimes such as drug trafficking, money laundering, high-tech smuggling, and terrorism.[140] Countries have countered these laws by passing their own aimed at the United States.[141] This is particularly evident as the United States enforces its laws to combat money laundering by interfering with foreign bank secrecy laws.[142] The resulting clashes and retaliatory measures are the reasons why the United States has historically avoided interfering with the acts of foreign sovereigns. When feasible, treaties and multilateral agreements are more effective and prudent alternatives to sacrificing international comity.[143]

IV. LAW ENFORCEMENT DIFFICULTIES

Historically, technology has been a barrier to law enforcement. Today, law enforcement is still struggling to keep pace with the increasing sophistication of crime.[144] The new technologies that criminals use are

---

138. The United States has used a device termed a "compelled waiver" to obtain evidence extraterritorially in derogation of foreign secrecy protection. As Berta Hernandez describes:

> A compelled waiver, more commonly known as a consent directive, is a written form which sets forth an individual's consent to the disclosure of her/his foreign bank records. In short, the individual executes a written directive to the foreign bank to divulge information about her/his account to the Department of Justice. The individual's authorization is given under "compelled consent" because if the individual refuses to sign the directive, she/he can be held in contempt.

Berta Esperanza Hernandez, *RIP to IRP—Money Laundering and Drug Trafficking Controls Score a Knockout Victory over Bank Secrecy,* 18 N.C. J. INT'L L. & COM. REG. 235, 251 n.97 (1993).

The use of a compelled waiver does not violate the Constitution. *See* Doe v. United States, 487 U.S. 201 (1988) (holding that the compelled execution of a consent form directing the disclosure of foreign bank records does not implicate the Fifth Amendment privilege against self-incrimination because it is not a testimonial communication but akin to furnishing a blood sample).

139. *See* sources cited *supra* note 138.

140. Nadelmann, *supra* note 120, at 38. Note that the DEA has over 60 overseas offices and 200 agents stationed abroad. *Id.* at 39.

141. Davidson, *supra* note 123, at 119.

142. *See* C. Todd Jones, *Compulsion over Comity: The United States' Assault on Foreign Bank Secrecy*, 12 NW. J. INT'L L. & BUS. 454 (1992).

143. Many nations by treaty or through agreement permit the United States great latitude in law enforcement efforts. OFFICE OF TECHNOLOGY ASSESSMENT, U.S. CONGRESS, INFORMATION TECHNOLOGIES FOR CONTROL OF MONEY LAUNDERING 115-17 (1995) [hereinafter MONEY LAUNDERING]. There are multilateral treaties in effect that require mutual cooperation in prosecuting drug trafficking, terrorism, and other international criminal activities. *Id.*

144. *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on*

so sophisticated that some crimes are nearly undetectable by law enforcement.[145] Additionally, the substantial cost and time spent to secure evidence may enable criminals to escape prosecution.

Operators of virtual casinos will likely employ these new technologies to prevent law enforcement from viewing a casino or a gambler in the act of gambling. In order to view the activity, the law needs to intercept the communication between the casino and the individual. Since the casino operator probably would not give permission to view, law enforcement needs to intercept the communication by tapping the wires. For law enforcement to know which wire to tap in the United States, it first needs to trace the communication from the casino to a gambler within the United States.[146] Part IV.A. reveals the unique problems of tracing gamblers on the Internet. If the conversation is digitized, the law needs to convert the conversation and put the puzzle back together. To convert the conversation, law enforcement needs to know how the conversations were compressed and sent through various routes. Part IV.B. analyzes these barriers to wiretapping in the phone systems themselves. Law enforcement may need to decrypt the conversation.[147] Part IV.C. discusses encryption and shows how it can hide the gambling activity from law enforcement. Finally, to prove money was transferred for a gambling operation, law enforcement may need to break the protection involved in electronic money.[148] Part IV.D. explains electronic money and how it can hide gambling transactions. This complicated process may preclude law enforcement from effectively prosecuting an Internet casino if the laws remain unchanged.

A. Tracing on the Internet

Law enforcement's initial problem is in detecting the gamblers. This complication arises from the unique nature of the Internet; the gambler can hide his or her identity by using another name or disguising the source.[149]

Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103d Cong., 2nd Sess. 259 (1995) [hereinafter *Digital Telephony*] (statement of U.S. Dept. of Justice, Fed. Bureau of Investigation).

145. *Id.*

146. *See* discussion *infra* part IV.A.

147. *See* discussion *infra* part IV.D.

148. *See* discussion *infra* part V.C.

149. *See* Kelly Owen, *Speech on Internet Called Protected by Constitution*, L.A. TIMES, May 12, 1995, at A17; Adam S. Bauman, *Computer at Nuclear Lab Used for Access to Porn*, L.A. TIMES, July 12, 1994, at A1, A18.

Although this disguise is not foolproof,[150] unmasking it can be time consuming.[151] Time is critical in law enforcement, especially in detecting gambling; a gambler is unlikely to play these games for many hours. If the tracing takes longer than a few hours, tracing may not be possible.

Tracing is, at the most basic level, the process by which one asks a computer who is currently using that computer.[152] The computer returns a list of the addresess of who is using the computer.[153] However, if one is connected to the Internet without identification, e.g., through a university computer, the trace will only return the address of the computer being used.[154] Additionally, if the address of the user is somehow inaccurate, the user escapes discovery.[155]

B. Digital Telephony

Early wiretapping was relatively easy: all one needed to do was place alligator clips on the copper cables, which transmitted only analog signals.[156] However, much of the telephone communications today are digital, making law enforcement's early technology obsolete.

Digital telephony refers to the technical problems encountered in the phone systems themselves. Computers, faxes, and voice signals are converted into digital code and compacted for transmission over the telephone cables.[157] Thousands of machines and people transmit signals

---

150. Note how the infamous hacker Kevin Mitnick was caught. Mitnick broke into the computer system of computer security expert Tsutomu Shimomura on Christmas Day, stealing 20,000 files on security. Shimomura was able to trace Mitnick through the Internet. Claire Tristram, *Ten Things You Need to Know About . . . Firewalls*, OPEN COMPUTING, May 1995, at 61.

151. Jerome Day, Director of the Hong Kong Baptist University's Computing and Telecommunications Services Center, tells that the University's research and activities were infiltrated by a hacker. The University spent about 400 staff hours tracing the hacker and trying to discern evidence of who the hacker was. Benson Chao, *Academics Warned to Block Hackers*, S. CHINA MORNING POST, Mar. 30, 1995, at 15, 18.

152. *See e.g.*, MARTIN A. POYSER, FLEETSOFT TRACE MANUAL, http://fleetwood.salford.ac.uk /~fleetie/trace_manual.html (on file with *Loyola of Los Angeles Entertainment Law Journal*).

153. *Id.*

154. *Id.*

155. *Id.*

156. *See* Jaleen Nelson, Comment, *Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and Its Effect on Free Flow of Information and Privacy*, 41 UCLA L. REV. 1139, 1179 (1994).

157. Andrew Grosso, *The National Information Infrastructure*, 41 FED. B. NEWS & J. 481, 486 (1994).

from telephones to a location called the "exchange."[158] The exchange then attaches an identification code to each signal and combines these signals mathematically to maximize the use of telephone cables.[159] Sometimes different segments of the same phone transmission are diverted through several different routes.[160]

When law enforcement agencies attempt to wiretap, they receive not only the suspect's communication but also thousands of other communications, all coded and bundled mathematically in a digital packet.[161] The suspect's conversation is mixed into a mathematical mesh, which is useless to the officials.[162]

The FBI has convinced Congress to address the law enforcement concerns posed by digital telephony.[163] In October 1994, Congress passed the Communications Assistance for Law Enforcement Act.[164] The Act provides that telecommunications carriers must make their systems readily available for interceptions and tracing within at least four years, with some extensions permissible.[165] However, in the interim, and as telephone systems abroad go digital, digital telephony may present law enforcement with problems in gathering the evidence necessary to prosecute the Internet casinos for illegal gambling activity.[166] The law will be unable to put the puzzle back together—the pieces would be scattered throughout the country, and they would be mixed together with millions of pieces of other puzzles.

C. Encryption

The sounds of chips sliding across a craps table in the interactive Internet casinos can be hidden from law enforcement by means of encryption. Encryption is a technique by which one hides certain data from another by changing words into numbers and then performing math on the

158. *Electronic Surveillance in a Digital Age*, U.S. Cong., Office of Technology Assessment, OTA-BP-ITC-149, July 1995, at 39 [hereinafter *Electronic Surveillance*].

159. *Id.* at 58.

160. *Id.* at 57.

161. *Id.* at 35, 58.

162. *Digital Telephony*, *supra* note 144, at 273.

163. *Id.* at 259.

164. Communications Assistance for Law Enforcement Act, PUB. L. NO. 103-414, § 101, 108 STAT. 4279 (1994) (to be codified at 47 U.S.C. § 1001).

165. *Id.* § 104.

166. *Digital Telephony*, *supra* note 144, at 270.

numbers to create new numbers.[167] The key to encryption is that one needs to know the formula employed to make sense of the numbers.[168]

With encryption, banks protect themselves from theft.[169] This protection allows individuals the convenience of automated teller machines ("ATMs") which use encryption to protect financial transactions.[170] Similarly, businesses use encryption to protect trade secrets.[171]

---

167. D.C. Toedt, *Encryption: An Inexpensive Alternative to Escrow?*, THE COMPUTER LAW., Nov. 1994, at 19.

168. There are two main types of encryption: public key (i.e., DES) and private key (i.e., RSA). DES (Data Encryption Standard) was developed by IBM in the mid-1970s with help from the National Security Administration. Ira S. Rubenstein, *Export Controls on Encryption Software*, COPING WITH U.S. EXPORT CONTROLS, Oct. 1994, at 177, 183-84. It was designed and originally classified as protection for "unclassified but sensitive" information. *Id.* at 184. There is a weakness in private key encryption: the parties must tell each other what the secret encrypting number is. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 890 (1995). Thus, the encryption is only as strong as the protection given to the transfer between the parties of that encryption code. A mathematical trick exists that allows both sides to give each other that key or entry code without revealing it publicly, based upon computational times. Rubenstein, *supra* at 184. This mathematical trick delays the communication between the parties, and relies upon several back and forth communications, which may be impractical. *Id.* at 183-84.

In public key encryption (DES) the two keys or entry codes are mathematically related. *See* Froomkin, *supra* at 893. One code, the public key, is available for everyone to see, know, and possess. *Id.* at 891. The private key is kept secret. *Id.* at 887. One can only decrypt the text with the private key of the receiver. To break the secret, private key or code, one must either find a weakness in the formula which encrypted the communication, get the private key by its having been revealed or stolen, mathematically discern the private key from the public key, or try every single number until one works. *Id.* Finding a weakness in the formula is sometimes possible.

Mathematically discerning the private, secret key is difficult and may be time prohibitive. For example, banks when transmitting money through the phone lines for ATM machines use a short number only eight characters long. An eight character key can be cracked by the National Security Agency in a minimum twenty minutes, as there are only seventy-two quadrillion possible combinations. Froomkin, *supra* at 833. This is the process that Damien Doligez used in August of 1995 to crack the code that Netscape had assured security to its consumers. *See* Gary H. Anthes, *Lack of Security Is No Obstacle*, COMPUTERWORLD, Aug. 28, 1995, at 59. The encryption attacked was RSA Data Security's RC4 which was the maximum encryption strength allowed to be exported out of the United States by munition rules. *Id.* There were about one trillion permutations of the forty bit security code. *Id.* Doligez linked 112 university computers in a "brute force" search and cracked the code in fifteen days. *Id.*

169. Banks use DES. *Bankers Try to Hang on to an Old Security Friend*, BANK NETWORK NEWS, Aug. 11, 1995, *available in* LEXIS, News Library, Cumws file.

170. Froomkin, *supra* note 168, at 720. In the United States each day, Fedwire and the Clearing House Interbank Payment System transfer an estimated one to two trillion dollars using encryption. *Id.* at 719.

171. *Id.* at 722. In 1993, $130 billion was spent on nongovernmental research and development. *Id.*

Encryption also can be an illegal casino operator's dream come true and law enforcement's worst nightmare.[172] Casino operators may use encryption to hide their activity and protect the identity of their users from the authorities.[173] Because of the potential for abuse, the federal government has tried to impose strict control over encryption technology.[174] However, the government's control over encryption technology has been a near failure. One can easily and without any governmental interference find and use encryption on the Internet.[175]

---

172. According to Steven Levy, an expert in encryption and computer crime, encryption is:

> the National Security Agency's greatest nightmare. Every company, every citizen now [has] routine access to the sorts of cryptographic technology that not many years ago ranked alongside the atom bomb as a source of power. Every call, every computer message, every fax in the world could be harder to decipher than the famous German 'Enigma' machine of World War II. Maybe even impossible to decipher!

Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES MAG., June 12, 1994, at 46, 48.

173. In fact, encryption is already being used to hide activity from law enforcement. Peter H. Lewis, *The F.B.I. Sting Operation on Child Pornography Raises Questions About Encryption*, N.Y. TIMES, Sept. 25, 1995, at D5. On September 13, 1995, federal agents searched more than 125 homes and offices throughout the United States to seize computers and diskettes of suspected traffickers in child pornography. *Id.* However, only fifteen arrests were made as of September 25, 1995 because the traffickers had encrypted the pictures, which law enforcement was not able to break. *Id.* One professor of computer science tells of over twenty cases regarding child pornography, terrorism, murder, embezzlement, fraud, tax protests, and export violations where encryption proved difficult for law enforcement. *Id.*

174. The federal government classifies encryption technology as a United States munition, like a tank or a fighter jet. 22 C.F.R. § 121.15 (1994). Although restrictions on the export of encryption technology were eased, the exportation is still highly controlled and limited. Rubenstein, *supra* note 168, at 219.

175. RSA Data Security offers for free its version of RSA encryption at http://www.rsa.com/rsa/prodspec/rsasec/sec_eval/ (available as of Mar. 23, 1996).

DES software can be anonymously downloaded from the Internet and is available in at least 166 products. Rubenstein, *supra* note 168, at 185. One solution proposed by the Clinton administration was to mandate the use of the government's own encryption technology. The federal government's encryption products are called the Clipper Chip and Capstone. Christopher E. Torkelson, Comment, *The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment*, 25 SETON HALL L. REV. 1142 (1995); Timothy B. Lennon, Comment, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 Be Like 1984?*, 58 ALB. L. REV. 467, 502 (1994). The Capstone Chip was created to encrypt high-speed data transmissions, like those of computers and fax machines, and the Clipper Chip for low speed data and voice conversations. Nelson, *supra* note 156, at 1140. This encryption involves both hardware and software components to provide what the government terms, an unbreakable encryption, which the government wanted every government agency, business, and individual to use. Torkelson, *supra* at 1143. In return for government protection, the government would retain a key for law enforcement in order to intercept communications. Nelson, *supra* note 156, at 1164-65. However, there were widespread fears of government invasion of privacy and unlawful search and seizures, as well as resting all security interests on one encryption. In late May 1994, an AT&T researcher uncovered a significant flaw that allowed a bypass of the security protection. Levy, *supra* note 172, at 47. As a result, the project has not been adopted and consequently, the

Encryption potentially poses a serious threat to law enforcement. If the authorities are not able to determine that an individual is gambling because the individual's activity is enshrouded in code, that individual is immune from detection and thus from prosecution. Similarly, encryption also provides a cloak for the casinos. However, undercover agents may gain access to the Internet casinos, posing as gamblers, but issues of entrapment may arise.[176]

Encryption raises some significant problems. If law enforcement cannot prosecute gamblers because of encryption, then the laws against individuals gambling over the wires will have lost all force. The harm that these laws are designed to protect against—racketeering and organized crime—may resurface.

D. Electronic Money

Another significant barrier to the detection of Internet gambling is the use of new, untraceable and undecipherable financial transactions.[177] Protection of electronic transactions is important because greater protection promotes electronic commerce.[178] However, undecipherable financial transactions may also be an effective technique that casino operators and gamblers can use to hide evidence that money was transferred between them. Electronic transactions may be hidden on the Internet in several ways.

---

government's encryption products are nearly powerless against the more advanced ones. *Id.*

176. Entrapment theories and case analogy to entrapment are beyond the scope of this Comment, though they pose interesting enforcement questions.

177. *See* Kelley Holland & Amy Cortese, *The Future of Money*, BUS. WK., June 12, 1995, at 70.

178. One researcher notes that "the electronic agora is open, but few are shopping." David Bennahum, *The Trouble with E-cash*, MARKETING COMPUTERS, Apr. 1995, at 25. He notes this may change with a safe medium of exchange, such as E-cash. *Id.* According to James G. Cosgrove, vice-president and general manager for multimedia services at AT&T, "electronic commerce will literally change the way business is done worldwide . . . . We're about to see another revolution similar to the Industrial Revolution." Holland, *supra* note 177, at 66. Growth and profit potential has many companies researching and making plans for rapid implementation of electronic money. The Commerce Department estimates that $2.95 trillion will be spent electronically by the year 2005. *Id.* at 70. Citicorp is developing an Electronic Monetary System to be used by retail and business customers (including other banks) as an infrastructure for electronic transactions. *Id.* at 74.

1. The Techniques

a. Encrypting the Credit Card Number

One way to protect the secrecy of transmissions is through encryption.[179] This allows credit card numbers to be sent over the Internet without fear of interception.[180] The weakness of this method is in the strength or weakness of the encryption.[181] Anonymity is not a priority in this secured transaction because this form of transaction leaves records through credit card receipts.

b. Establishing Anonymous Numbered Bank Accounts

A second form of secured electronic transaction is similar to a Swiss bank account.[182] The gambler and the casino operator each set up bank

---

179. Mihir Bellare et al., *iKP—A Family of Secure Electronic Payment Protocols*, FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE 89 (1995).

180. Two companies, CommerceNet (CyberCash) and Netscape, provide encryption protection for these transactions. Peter E. Dyson, *Toward Electronic Money: Some Internet Experiments*, THE SEYBOLD REP. ON DESKTOP PUBLISHING, June 10, 1995, at 3. For example, if a gambler wishes to wager on an Internet casino, he or she would fill out a computer invoice with his or her credit card number or ATM PIN and the computer program encrypts the invoice such that only the casino can decrypt the invoice. The Internet casino decrypts the invoice, verifies the credit card or the Automated Teller Machine PIN, sends a receipt, and allows the wagering to proceed. *Id.* ATMs were introduced in the early 1970s following the introduction of credit cards. Originally, ATMs allowed withdrawals from only the customer's bank. As customers began to demand more convenience, banks developed ATM networks. In an ATM network, a third party processor performs the switching function that connects all the banks together. In the United States today, there are approximately 60 ATM networks. At the end of each day the banks settle accounts among themselves. *House Banking Domestic and International Monetary Policy Innovations in Currency: Hearings Before the Subcomm. on Domestic and International Monetary Policy of the House Comm. on Banking and Financial Services*, 1995 WL 441370 (statement of David M. Van Lear, Chairman and Chief Executive Officer, Electronic Payment Services, Inc.). A PIN is a several digit changeable password selected by the holder of a debit card to insure that only those who are authorized to withdraw money from a bank account can do so. *Id.*

181. Wells Fargo Bank is requesting that 100-bit encryption, rather than the 40-bit in place today, be used to secure ATM transactions on the Internet. Kim S. Nash & Thomas Hoffman, *Banks Hit Info Highway at Different Speeds; Rivals at Odds Regarding Internet Security, Acceptance*, COMPUTERWORLD, Aug. 21, 1995, at 52.

182. Article 47 of the banking code of Switzerland prohibits disclosure of any secrets entrusted to an officer of a bank, learned in his or her capacity as an officer. Hernandez, *supra* note 138, at 242. This requirement is founded on the Swiss' fundamental and historical beliefs in the invulnerability of privacy in banking and agency law. *Id.* at 244. Violation of the privacy can result in civil liability in tort, banking, and criminal law. *Id.* However, in 1990, Switzerland passed legislation that criminalizes obstruction of investigations into criminally derived assets.

accounts, identified only by number. The gambler then encrypts a message, including the gambler's bank account number, access code, amount to be transferred, and the recipient's bank account number.[183] Upon decrypting the message and verifying the access code, the bank then transfers the money between accounts.[184] If the bank or casino does not keep records regarding to whom the accounts belong or who is making the transaction, the transaction itself is not traceable. An Internet casino could use this technique to hide its transactions from law enforcement. Requiring that each customer have a numbered bank account, however, may prevent the widespread use of this type of financial transaction; establishing numbered accounts involves some inconvenience.

c. Third Party Escrow

A third technique is labelled third party escrow.[185] This technique involves a third party who handles the billing and crediting.[186] Both the gambler and the casino establish accounts with the third party.[187] These accounts are then linked to the customer's or casino's traditional bank.[188] When an offer to gamble is accepted, the respective accounts are debited and credited accordingly. The account holders are not anonymous, as the third party keeps complete records of the parties involved and the amounts transferred.[189] However, the nature of the transaction is not released to the third party.[190] Although this scheme may afford gamblers some protection, when one of the parties is "Virtual Vegas" it may be relatively simple to infer the nature of the transactions. Additionally, were the third

---

This prohibits officers, within the scope of their profession, from accepting third party funds without verifying the owner's identity. *Id.* at 276.

183. Glyn Moody, *Spending Your Money Safely on the Internet: How to Find a System That Will Allow You to Pay for Goods While Guaranteeing Secure Transfer*, COMPUTER WKLY., July 13, 1995, at 39.

184. *Id.*

185. *See* CARNEGIE MELLON, NETBILL, http://www.ini.cmu.edu/NETBILL/home.html (updated May 15, 1995) (on file with *Loyola of Los Angeles Entertainment Law Journal*); Benjamin Cox et al., *NetBill Security and Transaction Protocol*, FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE 77 (1995).

186. L. Jean Camp et al., *Token and Notational Money in Electronic Commerce*, FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE 1, 9 (1995).

187. Cox, *supra* note 185, at 77.

188. *Id.*

189. Camp, *supra* note 186, at 9.

190. *Id.*

party's server infiltrated, the account information privacy might be compromised.[191]

d. Electronic Cash

The fourth technique, which is the most novel and complicated, involves an entirely new type of currency[192] which is sometimes called electronic cash, E-cash, or "E$."[193] If a gambler wishes to wager on an Internet casino by using E-cash, he or she would press "pay $100" and the bank would credit the casino's account.[194] This transaction is secured through layers of encryption.[195] The gambler's identity, the casino's identity, and quantity of money transferred are kept secret from law enforcement because E-cash precludes identification through mathematical formulas.[196] The advantage of E-cash is that each party involved—the casino, the bank, and the gambler—is able to keep secret his or her identity and the amount transferred. The information is all kept together in a mathematical mesh.[197]

---

191. *Id.*

192. David K. Gifford et al., *Payment Switches for Open Networks*, FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE 69 (1995).

193. DigiCash is the best known company using this form of secured financial transaction. *See* DigiCash, *supra* note 7.

The bank, in exchange for hard currency, gives the buyer of electronic currency a serial number encrypted with one of the bank's secret keys. The bank may use different keys for different currency denominations. The bank then publishes the corresponding public keys such that a vendor can verify the denomination because only the public key of a particular denomination will unlock the encryption. *See* Dyson, *supra* note 180, at 12. DigiCash works by using layers of encryption. The user encrypts his or her serial number to hide it from the bank, so that only the user can decrypt the code to prove the serial number. The user finally encrypts with his or her private key the bank-encrypted denomination and the encrypted serial number, so that anyone with the public key can decrypt the money. *Id.*

194. This program is either the Netscape Web browser, which is available in most computer stores, or the CyberCash Web browser, which is available at http://www.cybercash.com /cybercash/product/get_wallet.html/ (available as of Mar 23, 1996); Dyson, *supra* note 180.

195. *See* Digicash, About E-Cash http://www.digicash.com/ecash/about.html (spot [2d hit]: security) (on file with *Loyola of Los Angeles Entertainment Law Journal*).

196. The bank knows that the currency is valid because it recognizes its signature encryption. It subtracts the amount requested from a running balance in a client's numbered bank account. *Id.*

197. *Id.*

e. Stored Value Cards

The fifth technique is called a smartcard or stored-value card. These cards are equipped with a microprocessor that stores the value of currency on the card as well as secret codes for protection.[198]

These cards are swiped like credit cards or ATM cards, and they keep a running balance.[199] Because there may be no picture printed on the card and the records produced by its use may be unclear, the audit trail is weak.[200] The gambler and casinos may be able to hide their transactions.[201]

2. Law Enforcement Difficulties

With the growth of electronic currency comes many related problems: system integrity, regulation, authentication, tracking money supply, taxability, auditability, fraud control, and sovereignty issues.[202] Gamblers, gambling organizations, and money launderers may be aided in hiding their transactions by cyberspace banking in three ways: placement, layering, and integration.[203] Launderers want to place their money in legitimate repositories such as banks, securities, or real estate.[204] Conventional banks in the United States keep detailed records as required by federal law.[205] Cyberbanks do not. Thus, federal lawmakers and law enforcement should consider extending federal banking and credit regulations to encompass these international electronic currency transactions.[206]

Money launderers also try to move their assets through layers of transactions to hide the illegal source.[207] The more layers through which

---

198. Bennet Yee & J.D. Tygar, *Secure Coprocessors in Electronic Commerce Applications*, FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE 155 (1995); Leslie Helm, *Cashless Society Gets Closer with Plans for Electronic Currency*, L.A. TIMES, Sept. 6, 1995, at D4.

199. Yee & Tygar, *supra* note 198, at 155; Helm, *supra* note 198, at D4.

200. *Electronic Payment Law Caution Urged*, L.A. TIMES, Oct. 12, 1995, at D3.

201. *Id.*

202. *See generally* MONEY LAUNDERING, *supra* note 143.

203. *Id.* at 3-4.

204. *Id.* at 1-10.

205. *Id.* at 37. For example, financial institutions are required to submit Form 4789 (Currency Transaction Report ("CTR")) for all cash transactions of $10,000 or more. *Id.* In 1994, 10,765,000 CTRs were filed. MONEY LAUNDERING, *supra* note 143, at 7.

206. A discussion of federal banking and credit regulations and their applicability to the Internet is beyond the scope of this Comment. However, the issues raised are important to the future of law enforcement and the banking and credit industries.

207. MONEY LAUNDERING, *supra* note 143, at 8-10.

the transactions pass, the harder the source is to trace.[208] Gambling organizations may hide the funds deposited in their numbered cyberspace accounts[209] or their untraceable E-cash by moving these assets through various legitimate sources like securities or commercial purchases.[210] Cyberspace banking through anonymous electronic money may complicate the detection of illegal money because such money has been layered with apparently legitimate transactions.

Finally, launderers attempt to turn illegal money into "clean" money.[211] Cyberspace banking may allow direct anonymous cash withdrawals.[212]

The Treasury Department has attempted to detect the international laundering of money through a comprehensive computer database.[213] In 1990, Treasury Secretary Nicholas Brady established the Financial Crimes Enforcement Network ("FinCEN") to detect financial crime.[214] Its mission was: "(1) to gather financial and related records and data from federal, state, local, and foreign agencies; (2) to analyze collected records for evidence of money laundering and other financial crimes; and (3) to disseminate its findings to law enforcement agencies in the United States and abroad."[215]

Currently, FinCEN applies an artificial intelligence system that uses certain rules to detect suspicious activity.[216] These rules are designed to emulate the thought processes of expert investigators.[217] This comprehensive database includes reports of domestic and international transactions greater than $10,000, large winnings at casino tables, purchases greater than $10,000, reports of suspicious transactions over $1000, European crime files, driver's license information, credit bureau data, and various other public and private filings.[218]

---

208. Emily J. Lawrence, *Let the Seller Beware: Money Laundering, Merchants and 18 U.S.C. §§ 1956, 1957*, 33 B.C. L. REV. 841, 849 (1992).

209. *See* discussion *infra* Part IV.D.1.b ("Numbered bank accounts").

210. MONEY LAUNDERING, *supra* note 143, at 9.

211. *Id.* at 2.

212. Holland & Cortese, *supra* note 177, at 78.

213. Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?*, 34 JURIMETRICS J. 383, 392 (1994).

214. *Id.* at 389-90. FinCEN has a staff of 200 computer and money laundering experts. *Id.* at 391. The database was used to trace $1 billion in drug sales to 683 accounts in 37 Panamanian banks and to freeze 11 bank accounts, $3.5 million in real estate property and other assets belonging to suspected fronts for Saddam Hussein. *Id.* at 392.

215. *Id.* at 389-90.

216. MONEY LAUNDERING, *supra* note 143, at 43.

217. Bercu, *supra* note 213, at 394.

218. *Id.*; *see* MONEY LAUNDERING, *supra* note 143, at 45.

Cyberbanking, lacking a traceable audit trail, poses a significant threat to FinCEN's integrity and the ability of law enforcement to prosecute gamblers and Internet casinos. FinCEN recently had a colloquium to come up with suggestions and recommendations to address these concerns.[219] The director of FinCEN notes:

> The new systems combine the speed of the present bank-based wire transfer system with the anonymity of currency—they create the best of both worlds. They make wire transfer equivalents anonymous, and they make currency easy to move around the world at almost the speed of light. Smart card transactions and international payments transacted over the vast Internet system could be immediate, potentially anonymous, effected in multiple currencies, and conducted entirely outside of the traditional funds transfer channels.[220]

However, Morris cautions that stored value cards may also allow sophisticated criminals to hide their money in locations around the world through an unlimited number of smart cards—"all anonymously, all without an audit trail, and all without the need to resort to a traditional financial institution."[221] Already $300 billion is estimated to be laundered annually from the United States.[222] With an increase in the use of anonymous Internet currency or smartcards, this amount is destined to increase.

These new forms of Internet currency may be a tremendous boon to Internet commerce. However, if unchecked, criminal activity and gambling may reign supreme over the law. Safeguards such as placing restrictions on anonymous currency, numbered bank accounts, and anonymous stored value cards may be an appropriate move to protect the integrity and effectiveness of law enforcement.

V. SOLUTIONS

Although federal law seems to prohibit Internet gambling, laws which aim at the casinos are ineffective due to jurisdictional concerns and

---

219. *United States Department of the Treasury Before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services, United States House of Representatives*, Oct. 11, 1995, *Comments of Stanley E. Morris, Director of the Financial Crimes Enforcement Network (FinCEN)* [hereinafter *Banking*]; *Banking, Bill's EFTA and Reg E Exemptions Need Reworking, Blinder Tells Panel*, DAILY REP. FOR EXECUTIVES (BNA), Oct. 12, 1995, at 197.

220. *Banking*, *supra* note 219, at 200.

221. *Id.* at 201.

222. MONEY LAUNDERING, *supra* note 143, at 2.

enforcement difficulties. This section discusses three possible solutions that would either control or eliminate the growth of Internet gambling. First, Internet gambling may be eliminated by requiring domestic Internet access providers to block access to the Internet casinos or face civil liability. Second, Internet gambling can be controlled with legalization coupled with the prohibition of access by minors. Finally, Internet gambling can also be controlled by equipping families with the necessary technology to block access.

A. Civil Liability on Access Provider—Block Access Entirely

Gambling in any shape or form produces fallout resulting in addiction, crime, and social disruption. Usually the social costs of regular casinos are said to be outweighed by the economic benefits it brings. However, the social costs of Internet gambling may not be outweighed by the economic benefits because the revenue produced by Internet gambling would most likely be transferred to other countries. Consequently, the United States, as a society, is left with the burden of the hidden social and economic costs without much revenue in return.

Because the laws against Internet casinos and those who wager on the Internet have been shown to be ineffective,[223] one possible solution is to block access to these casinos by holding the access providers, located in the United States, liable for allowing access through their service. This solution is similar to Senator J. James Exon's (D-Nebraska) first proposal in regulating obscenity on the Internet.[224] The Exon Bill originally held access providers liable for the transmission of obscene materials on their services.[225] If such transmissions were found, the provider would be subject to a $100,000 fine or a two-year imprisonment term or both.[226] This bill required access providers, such as America Online, to police their postings.[227] If the providers were held liable for allowing access to illegal gambling, then the jurisdictional, international comity, and law enforcement problems would be virtually eliminated.

---

223. *See* discussion *supra* part IV.

224. S. 314, 104th Cong., 1st Sess. § 2(b) (1995).

225. *Id.* The revised Exon Bill removed the penalties against access providers for mere transmission. S. 652, 104th Cong., 1st Sess. § 402 (1995). The Exon Bill, now incorporated into the Telecommunication Competition and Deregulation Act of 1996, continues to criminalize posting or soliciting of material that is "obscene, lewd, lascivious, filthy or indecent." Telecommunication Competition & Deregulation Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 56, 133.

226. S. 314, 104th Cong., 1st Sess. § 2(b) (1995).

227. *Id.*

1. Jurisdiction and International Comity

By holding access providers who are located in the United States liable for allowing casinos to be used through their service, the jurisdictional problem would be solved. Each state has general jurisdiction over the providers because the providers have sufficient contact with each state. Not only are they physically present in each state, but they also direct their activities to the states through their advertisements and services. This creates general jurisdiction over the access providers.

However, if general jurisdiction was not achievable, specific jurisdiction would certainly exist. The advertisements and services are not sporadic or attenuated, but substantial. Thus, the providers' due process rights would not be violated if those states in which providers have services exercise specific jurisdiction over them. Furthermore, the issue of international comity does not even arise because the access providers are located in the United States.

2. Law Enforcement

The problems with law enforcement would also be resolved if providers were held liable because they would be forced to police their own services to avoid the penalties. This task would not be overly burdensome because the technology already exists for providers to proscribe access to certain types of service.[228] This is evidenced by CompuServe's recent cut off of access to 200 sexually oriented adult bulletin board services after German prosecutors claimed that the material violated Germany's pornography laws.[229]

To further prevent the law from being overly burdensome, the law should not be overly restrictive. It should only require the providers to make a good faith effort at blocking Internet gambling. Thus, if an Internet casino was somehow able to circumvent the blocking mechanism, then the provider should not be held civilly liable.

Users can also play a role in law enforcement. Not only could users report Internet gambling activity to the authorities, but if the authors' proposed changes to the laws were enacted to make access providers civilly

---

228. Mary Willians Walsh, *2 Views on 1st Amendment: As Americans Decry What They See as Online Censorship, Germans Wonder What All the Fuss Is About*, L.A. TIMES, Mar. 13, 1996, at D5, D7.

229. *Id.* CompuServe has since allowed access to most of these adult bulletin boards and is providing new filtering options. *Id.* at D7.

liable, users could also bring civil suit, in conjunction with the Justice Department, against the providers. The users would be entitled to a percentage of the judgment rendered against the providers. Thus, Congress should set the fine large enough to serve as an incentive for users to enforce the law.

Holding access providers civilly liable may halt the proliferation of Internet gambling in the United States. However, this type of restriction may be overly broad. The possible effect of this restriction may not only be the ban of Internet gambling, but may also include the ban of sports scores and odds that may be used to assist a gambler in wagering. For this reason, a more narrowly tailored solution which legalizes Internet gambling with the condition that the casinos restrict access by minors may be preferable.

B. Legalize Internet Gambling with Some Restrictions

Conditional legalization is similar to a contract. Under this scheme, the United States grants the privilege of accepting wagers through the Internet, but only on the condition that the casinos submit to United States law and devise a system that prohibits minors from accessing the services to mitigate the growth of underage gambling.[230] For instance, the casinos could require gamblers to certify that they are over twenty-one years old. After the certification is verified, the casino could issue a secret code that enables players to log on.

Critics of legalization argue that legalized gambling will significantly and detrimentally impact the players and their families through addiction. They argue that one of the main contributors to addictive gambling behavior is accessibility, and Internet gambling is extremely easy to access.[231] All a gambler needs is a computer, a modem, and a telephone line.

---

230. Despite the impact of Internet gambling on compulsive gamblers, the solutions suggested in this Comment do not cure this problem due to its complex nature. Compulsive gambling is a problem that is best dealt with by counseling. Although, one may argue that any panacea will help in the battle against the ills of gambling in general. However, if society wants to eliminate compulsive gambling entirely or any of the other social ills of gambling, then all gambling—and not just Internet gambling—should be prohibited. For a discussion of social problems associated with gambling, see Ronald J. Rychlak, *The Introduction of Casino Gambling: Public Policy and the Law*, 64 MISS. L.J. 291 (1995).

231. Lisa Dempster, *You Can Bet That Some People Will Be Caught in Gambling 'Net*, CALGARY HERALD, May 13, 1995, at A1.

On the other hand, gambling has moved from being "forbidden, illegal, [and] immoral . . . to becoming accepted, normal behavior."[232] Statistics show that more than half of Americans bet at least once on government-approved games of chance last year.[233] Such widespread acceptance of gambling demonstrates society's approval of gambling in general. Accordingly, regulations against Internet gambling would likely be against public sentiment. Furthermore, a strike against Internet gambling, but not against lotteries, horse racing, pari-mutuels, sports betting, bingo games, Native American reservation gambling, and the multitude of various other forms of wagering accepted across the country would be inconsistent.

Moreover, conditional legalization of gambling is consistent with most states' policies that favor gambling. Most states permit gambling in some form or another. For example, New York[234] and Connecticut allow national phone wagering on horse races;[235] Kentucky, Ohio and Pennsylvania allow in-state phone wagering;[236] Maryland allows bettors to wager on horse racing through the television screen.[237] In fact, one could argue that if a lottery is a form of gambling, then every state in the Union except Utah and Hawaii allows some form of gambling.[238]

Because gambling can be very lucrative, the proliferation of wagering options is not surprising.[239] States likely see Internet gambling as a

---

232. Christopher Smith, *Mom, Apple Pie . . . And Gambling? It's Turning All-American Gambling Is Becoming All-American*, SALT LAKE TRIB., May 15, 1995, at A1 (quoting Professor Authur Cosby of the University of Mississippi).

233. *Id.* Fifty-four percent of Americans bet at least once in state-run lotteries last year; 21% wager on lotteries every week and 35% buy lottery tickets each month; casinos attracted 24% of gamblers and the gambling rate for bingo games was 7%; and men gamble more than women and whites gamble more than non-whites. *Id.*

234. The New York Racing Association believes it has found a loophole in the Wire Act and is accepting telephone bets from at-home gamblers in other states. I. Nelson Rose, *Interstate Betting: A Lot of Laws, Some Little Loopholes*, CASINO EXECUTIVE, June 1995, at 22, 23.

235. Linda Kleindienst, *Gambling Officials Wonder How to Keep Money in State*, SUN SENTINEL, July 26, 1995, at 7A.

236. *Id.*

237. *See* Ross Peddicord, *New on TV: You Bet Your Horse*, BALTIMORE SUN, Dec. 15, 1994, at 1A.

238. William M. Bulkeley, *Feeling Lucky? Electronics Is Bringing Gambling into Homes, Restaurants and Planes*, WALL ST. J., Aug. 16, 1995, at A1, A5.

239. Some states have used out-of-state wagering on horse racing and lottery as a source of tax revenues. As more states allow interstate wagering, other states are feeling the squeeze from the lost revenue. Representatives from Florida's troubled pari-mutuel are saying that interstate and Internet gambling is costing them lost bets, which means lost tax revenues. (Pari-mutuel is a system of betting on races in which those backing the winners divide, in proportion to their wagers, the total amount bet, minus a percentage for the track operators and taxes. WEBSTER'S NEW WORLD DICTIONARY 1033 (2d ed. 1972)). To prevent revenues from diminishing any

source of additional revenue. If Internet gambling were legalized, the states could collect taxes from the gamblers and casinos as they establish themselves in the United States.[240]

With conditional legalization, there will be no jurisdictional concerns because the Internet casinos would have to submit voluntarily to the jurisdiction of the United States in order to have the privilege of transmitting their services into the United States. Furthermore, law enforcement concerns could be more extensively addressed by prohibiting the transmission of encrypted gambling activities, except for the transfer of money. Conditional legalization, however, would not be effective against those casinos that refuse to submit to United States jurisdiction and laws. Under those circumstances, access providers that knowingly allow such illegal transmission would be held liable.

C. Empowering the Family to Prevent Access by Minors

A third possible solution to combat Internet gambling is to empower the family with the ability to block access. This scheme is analogous to the proposal of Congressional Representative Christopher Cox (R-California) and Senator (then-Representative) Ron Wyden (D-Oregon) on regulating Internet pornography.[241] Congressperson Cox proposes that technology be developed for parents to prevent obscene material from coming into their homes.[242] The Internet Freedom and Family Empowerment Act, incorporated into the Telecommunications Competition and Deregulation Act of 1996, improves user control over computer information services.[243] The bill would preserve the present free market system where the Internet is "unfettered by State and Federal regulations."[244] In fact, the bill specifically states that "[n]othing in this Act shall be construed to grant any jurisdiction or authority to the [FCC] with respect to economic or content regulation of the Internet or other interactive computer services."[245] Instead of government regulation, the bill encourages the development of

---

further, Florida representatives are also looking into allowing telephone wagering on in-state and out-of-state horse races, and on jai-alai games. Kleindienst, *supra* note 235.

240. Telephone industries are racing each other to establish interactive gambling. As more and more corporations embrace gambling, Internet gambling will likely expand. *See* Dave Mayfield, *No Sure Bet: Firm Hopes to Set up Lotto-by-Phone,* VIRGINIA-PILOT & THE LEDGER-STAR, Dec. 18, 1993, at A1.

241. H.R. 1978, 104th Cong., 1st Sess. § 2 (1995).

242. *Id.*

243. *Id.*

244. *Id.*

245. *Id.*

blocking mechanisms that empower parents' ability to restrict their children's access to objectionable or inappropriate online materials.[246]

One example of a blocking technology would be similar to the proposed anti-violence chip, the "V-chip," for television.[247] An anti-gambling chip, the "G-chip," for computers, would allow parents to block out Internet services that offer gambling, and thus, prevent minors from gaining access to the virtual casinos. A blocking mechanism would also allow the Internet to develop without governmental interference.

The issues of jurisdiction and law enforcement are not raised by this solution because it does not require the application of any law. This solution allows parents to dictate what activities are appropriate for their children to access.

VI. CONCLUSION

Internet gambling has no borders. Gambling activities flow freely and easily from one country to another. Although Internet gambling is illegal, trying to regulate this form of gambling with the current statutes would be like "performing brain surgery with stone tools"[248] because of the jurisdictional concerns and the law enforcement problems. First, the laws were designed for more traditional gambling establishments. Second, applying the antiquated notions of personal jurisdiction to the borderless Internet poses complex issues: have these casinos purposefully availed themselves of the jurisdiction of the United States? Do sufficient minimum contacts exit? Should the courts modify the traditional model of personal jurisdiction to adapt to the borderless Internet? Third, respect for international comity may preclude law enforcement from pursuing criminal action against the casinos because haling a foreign casino into United States courts may not be prudent for international relations. Fourth, the technology of modern crime is outpacing law enforcement's capability.

---

246. H.R. 1978, 104th Cong., 1st Sess. § 2 (1995); Senator Patrick Leahy (D-Vt.) takes a position similar to that of Congressperson Cox. The Senator believes that online pornography is a problem best addressed by parents, not the government. Empowering parents to screen children's computer activities is the best way to police the Internet without unduly restricting free speech or slowing the growth of this new communication system. Blocking technology would allow parents to decide which programs, from beer advertisements to pornography, they consider objectionable. Sen. Patrick Leahy, Congressional Press Releases, July 24, 1995, *available in* LEXIS, News Library, HILLPR File.

247. *See* Telecommunications Competition & Deregulation Act of 1996, Pub. L. No. 104-104, §§ 551-52, 110 Stat. 139-42.

248. I. Nelson Rose, *Wire Cops: The A.G.s Take on Internet Gambling*, CASINO EXECUTIVE, Aug. 22, 1995, at 22.

Encryption, digital communications, electronic cash, and tracing difficulties make enforcement of the current statutes against casinos virtually impossible.

The jurisdictional and law enforcement problems associated with Internet gambling can be avoided by holding the access providers liable. This solution eliminates the need for acquiring personal jurisdiction over casinos located abroad. Jurisdiction over the access providers would be general jurisdiction, as they are physically present in every state. Law enforcement problems will be eliminated because the providers themselves will block access to American customers from the Internet casinos.

Another possible solution is to combine conditional legalization with the use of blocking technology. This combination will better address the possible growth of underage gambling because both Internet casinos and parents will police access by minors.

Both solutions achieve their purpose: restricting access to Internet gambling. Which option is selected turns on your view of gambling. If you believe gambling over the Internet should not occur, holding the access providers liable is the most effective strategy. If you believe gambling over the Internet should be available, but believe that minors should be restricted from access, then conditional legalization with blocking technology is your most prudent choice. This evaluation is entirely subjective.

However, immediate legislative action is needed or law enforcement may lose what little opportunity it now has to make an impact.

Seth Gorman and Antony Loo[*]

* The authors sincerely thank the staff and editors of the *Loyola of Los Angeles Entertainment Law Journal* for their extreme dedication and invaluable help and suggestions. Antony Loo wishes to dedicate this Comment to his wife for her loving support. Both authors can be reached for question or comment at sethgorman@aol.com and aloo@aol.com.