

Can Internet Gambling Be Effectively Regulated? Managing the Risks

Authored by

Malcolm K. Sparrow

*John F. Kennedy School of Government
Harvard University*

With Contributions by

Coleman Bazelon, PhD

Charles Jackson, PhD

November 10, 2009

TABLE OF CONTENTS

I.	OVERVIEW OF APPROACH AND SUMMARY OF RESULTS	1
A.	Our Approach.....	2
1.	Gambling by Minors	2
2.	Criminal and Fraudulent Behavior.....	2
3.	Network Access, Data Privacy and Security Issues.....	3
4.	Problem Gambling.....	4
B.	The Status Quo Offers No Effective Protection	4
C.	Legalization and Regulation Would Afford Significantly Better Protection than the Status Quo.....	6
D.	Regulatory Methods and Technologies for Controlling Each Type of Risk Already Exist.....	7
1.	Gambling by Minors	9
2.	Criminal and Fraudulent Behavior.....	9
3.	Network Access, Data Privacy and Security Issues.....	11
4.	Problem Gambling	12
E.	Conclusions.....	15
II.	REGULATORY METHODS AND TECHNOLOGIES AVAILABLE FOR CONTROLLING EACH RISK	16
A.	Gambling by Minors	16
1.	The Issue of Gambling by Minors	16
2.	Existing Controls in Other Jurisdictions	17
3.	Relevant Technologies for Risk Mitigation	20
4.	Conclusion	23
B.	Defrauding of Consumers by Site Operators	24
1.	The Issue of Fraud by Site Operators	24
2.	Existing Controls in Other Jurisdictions	26
3.	Relevant Technologies for Risk Mitigation.....	28
4.	Conclusion	29
C.	Cheating or Defrauding of Players by Other Players.....	29
1.	The Issue of Players Being Defrauded by Other Players.....	29
2.	Existing Controls in Other Jurisdictions	31
3.	Relevant Technologies for Risk Mitigation.....	32
4.	Conclusion	33
D.	Involvement of Organized Crime in Gambling Operations.....	33
1.	The Issue of Involvement of Organized Crime in Online Gambling.....	33

2.	Existing Controls in Other Jurisdictions	34
3.	Relevant Technologies for Risk Mitigation	36
4.	Conclusion	36
E.	Money Laundering by Players	37
1.	The Issue of Money Laundering by Players	37
2.	Existing Controls in Other Jurisdictions	39
3.	Relevant Technologies for Risk Mitigation	40
4.	Conclusion	42
F.	Money Laundering by Site Operators	43
1.	The Issue of Money Laundering by Site Operators	43
2.	Existing Controls in Other Jurisdictions	44
3.	Relevant Technologies for Risk Mitigation	44
4.	Conclusion	45
G.	Violation of Jurisdictional Restrictions or Prohibitions	45
1.	The Issue of Violation of Jurisdictional Restrictions	45
2.	Regulatory Strategy	46
3.	Relevant Technologies for Risk Mitigation	47
4.	Conclusion	49
H.	Breaches of Data Confidentiality	50
1.	The Issue of Data Confidentiality	50
2.	Existing Controls in Other Jurisdictions	51
3.	Relevant Technologies for Risk Mitigation	52
4.	Conclusion	53
I.	Communications and Computer Security Failures	53
1.	The Issue of Communications and Computer Security Failures	53
2.	Existing Controls in Other Jurisdictions	55
3.	Relevant Technologies for Risk Mitigation	56
4.	Conclusion	58
J.	Problem Gambling	59
1.	Problem Gambling	59
III.	SPECIAL ATTENTION TO PROBLEM GAMBLING	60
A.	Introduction	60
B.	What is Problem Gambling?	60
1.	Terminology	60
2.	Prevalence Rates and Trends	61
C.	Potential Effects of Legalization of Online Gambling on Problem Gambling	62
1.	Potential Adverse Effects of Legalization	63

2.	Potential Benefits of Legalization.....	69
D.	Concluding Remarks.....	72

Acknowledgements

The authors would like to thank Dorothy Robyn, PhD, who contributed to this project while at The Brattle Group. The authors would also like to thank Pallavi Seth, PhD, and Michael Sutcliffe of The Brattle Group for their assistance.

About WiredSafety

This study was commissioned by WiredSafety.org, a 501(c) (3) charity and the largest and oldest online safety, education, and help group in the world. Originating in 1995 as a group of volunteers rating websites, it now provides one-to-one help, extensive information, and education to cyberspace users of all ages on a myriad of Internet and interactive technology safety issues. WiredSafety works in four major areas: help for online victims of cybercrime and harassment; assisting law enforcement worldwide on preventing and investigating cybercrimes; education; and providing information on all aspects of online safety, privacy and security. WiredSafety also has a longstanding interest in gambling policy and the prevention of underage gambling. The study was sponsored by Harrah's Operating Company, Inc and the Poker Player Alliance, who share many of WiredSafety's concerns. While the sponsors have provided valuable input into the framing of the research, the final decisions regarding the research approach and the final written product was solely made by the authors of the study, following consultation with WiredSafety, ensuring that the study was independent.

EXECUTIVE SUMMARY

This study was commissioned by Wired Safety, an Internet Safety and Educational charity. It examines a range of harms potentially associated with online gambling, and alternative methods for mitigating or minimizing them. Recognizing that the current U.S. prohibitionist regime with respect to online gambling is largely ineffective in achieving its aims, and provides no platform or opportunity for the implementation of most of the relevant harm-reduction strategies, we find that an alternative regime of legalization and regulation of online gambling would likely improve consumer welfare and protections. The body of this report evaluates a range of strategies, both regulatory and technological, that could be used to mitigate potential harms associated with online gambling more effectively.

Notwithstanding the current prohibitionist legal and regulatory approach, millions of U.S. residents gamble online through offshore gambling sites. As a result, the United States finds itself in the unfortunate position of incurring all the social costs of online gambling while having no control over the gaming sites that serve U.S. residents. The United States cannot disqualify industry participants from competing effectively for U.S.-based customers or offer its residents any consumer protections. Nearly all states permit some form of commercial gambling, and the industry is large and well-established. Clearly, policymakers have extensive precedent from which to draw strategies to mitigate the potential social harms of gambling.

Although some controls used in bricks-and-mortar casinos may not translate well to online gambling, several of the risks we examined become *more* amenable to control online. New technologies can be effective, even for those risks that are more difficult to address online. For example, geolocation and age verification technologies can help turn potentially significant risks into manageable ones.

In this study, we analyze 10 specific risks that others have suggested are potentially associated with online gambling: gambling by minors, fraud by operators, fraud by players, organized crime, money laundering by players, money laundering by operators, violation of jurisdictional prohibitions, breaches of data confidentiality, lack of site security, and problem gambling. It is important that regulators treat each of these potential risks differently. For some risks (such as players cheating other players), the public interest and the interests of the gaming industry align, making a cooperative regulatory relationship natural. For others (such as those involving potentially criminal conduct by operators), a strict enforcement regime would be more appropriate. Still other potential risks (such as underage and problem gambling) call for a more nuanced regulatory approach involving a mixture of strict enforcement, effective nonprofit support, community education, and cooperation, in keeping with the more complex motivations and incentives facing site operators.

For each of the 10 risks, we examined a set of regulatory methods and technologies that would provide a reasonable degree of risk management in a regulated environment. Most of these methods have already been implemented in some form in other jurisdictions. The United Kingdom, Alderney, Gibraltar, and others have successfully implemented

regulation, and nearly all of the well-regulated jurisdictions we studied address the 10 risks to some degree.

The establishment of a well-regulated industry under U.S. jurisdiction would offer far better protection against online gambling's potential social harms than outright prohibition. Combining a thoughtful regulatory scheme with education, technology tools, and support appears to be the most effective means of handling the realities and risks of online gambling in the United States. Therefore, we recommend that plans for regulating online gambling include the design and use of different risk-management strategies tailored to the different classes of risk that are associated with Internet gambling. In the end, consumers in the United States would be better protected than they are now.

I. OVERVIEW OF APPROACH AND SUMMARY OF RESULTS

Congress is debating legislation that would remove the existing prohibition on the use of the Internet for most types of gambling.¹ The proposed legalization of online gambling would be conditioned on the imposition of regulation designed to limit or prevent potential harms such as underage gambling, money laundering, and problem gambling.

A key issue in the debate over legalization of online gambling is whether regulation and technology could effectively control such potential harms. Some of the opposition to legalization reflects a perception that online gambling—in contrast to gambling in bricks-and-mortar casinos—would be difficult, if not impossible, to regulate effectively.

This study reviews the research literature and international approaches to online gambling. WiredSafety (the Internet safety and educational charity) has commissioned this study to help inform the legalization debate and to help educate the public on the risks associated with online gambling and the best ways to address those risks.

We note that our expertise is in regulatory policy and its relationship to risk analysis, rather than in any extensive prior knowledge of the gaming industry and gambling behavior per se. We have critically reviewed the existing literature, evaluated relevant technologies, and interviewed a range of scholars and practitioner experts, both here and abroad. We have not, however, conducted any new epidemiological studies or field research. Our distinctive contribution is the frame for risk management and regulatory analysis, rather than any new scientific inquiry.

Our analysis does not directly address whether online gambling should be legalized. In focusing on managing risks, we did not weigh moral or religious objections to gambling, nor did we examine broadly libertarian arguments in favor of allowing adults to engage in pastimes they may enjoy. We did not conduct any analysis to quantify the benefits of potential tax revenues attributable to regulated online gambling. Further, we have not focused on any issues of federalism or on exactly where regulations and laws should fit into the U.S. multijurisdictional governance structure. Instead, we concentrated more narrowly on the obligations of government to protect citizens in general, and vulnerable groups of citizens in particular, from unnecessary exposure to harm.

We sought (1) to identify the specific risks that are associated with, or perceived to be associated with, Internet gambling; (2) to determine suitable regulatory strategies for controlling or managing those risks; and (3) to assess how effective those strategies are likely to be. We identified 10 distinct risks that fall into four broad categories. Those categories are as follows:

¹ Internet Gambling Regulation, Consumer Protection, and Enforcement Act, H.R. 2267, 111th Cong. (2009), http://www.house.gov/apps/list/press/financialsvcs_dem/21frank_008_xml.pdf (last accessed on July 23, 2009), and Internet Gambling Regulation and Tax Enforcement Act of 2009, H.R. 2268, 111th Cong. (2009), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h2268ih.txt.pdf (last accessed on August 28, 2009).

- Gambling by minors
- Criminal and fraudulent behavior
- Network access, data privacy and security
- Problem gambling

On the basis of our review of the existing literature and interviews with academics, regulators, industry participants, and public interest advocates, we came to the following conclusions:

- Online gambling could be regulated effectively if it were legalized.
- A well-structured regulatory regime should provide much better social and consumer protections than the status quo for the risks we identified.
- At a minimum, even an imperfect legalization and regulatory regime for online gambling would give Americans much more protection than they have now. The current prohibitionist policy is extremely weak: large numbers of U.S. residents already gamble online, but they do so using offshore sites, many of which are poorly regulated or unregulated.

For each of the 10 risks we examined, a set of regulatory methods and technologies exist that would provide a reasonable degree of control, and most of them have been implemented effectively in other jurisdictions or in other online settings.

Although some controls used in the bricks-and-mortar environment may not translate to online gambling environments, several of the risks we examined become *more* amenable to control online. Comprehensive electronic records and the ability to track financial transactions and betting patterns provide more opportunities for analysis and audit, and hence improve the chances of discovering fraud or criminal activity. They also allow gambling websites to provide tools to mitigate problem gambling in a timely manner.

A. Our Approach

Our approach has been to identify the specific risks that are perceived to be associated with Internet gambling and then to determine how best to control or manage them. Those risks are described below.

1. Gambling by Minors

- a. Gambling by minors: There is concern that minors might find it easier to access and use online gambling services in a legalized environment.

2. Criminal and Fraudulent Behavior

- a. Defrauding of consumers by site operators: There is the possibility that online site operators may be more likely than their bricks-and-mortar counterparts to rig games, refuse to pay out

winnings, or simply vanish, taking with them players' account balances.

- b. *Cheating or defrauding of players by other players:* There is a concern that players could collude to defraud others, particularly in online poker. Online gambling may offer opportunities for collusion that are not available in a physical environment with visual surveillance.
- c. *Involvement of organized crime in gambling operations:* Organized crime has a history of involvement with the bricks-and-mortar casinos and is now involved in some online commerce. There is some concern that involvement in the online gambling industry may be a natural next step.
- d. *Money laundering by players:* There is concern that players or groups of players acting in concert could use legitimate gambling operations for money laundering.
- e. *Money laundering by site operators:* The possibility has been raised that site operators could use online gambling operations, with its significant financial flows, as a cover for money laundering on a large scale.

3. Network Access, Data Privacy and Security Issues

- a. *Violation of jurisdictional restrictions or prohibitions:* Government at the state, local, and tribal levels has traditionally exercised control over gambling within a given jurisdiction. The advent of the Internet has opened the question as to whether controls mandated by any proposed laws can be enforced within particular jurisdictions.
- b. *Breaches of data confidentiality:* To register for play, players surrender personal or financial data to site operators. Consumers might be harmed by deliberate or accidental breaches of the confidentiality of those data.
- c. *Communications and computer security failures:* Some are concerned that site operators might not use appropriate security practices, procedures, and technologies to ensure the integrity of their sites, the gaming on those sites, and player interactions. Absent proper security measures, malicious code could be transmitted to players, game operations could be infiltrated, and intrusions into the systems could compromise the game play and security of users.

4. Problem Gambling

- a. Problem gambling behaviors: Some argue that increased opportunity to gamble at any time, from anywhere, and at a faster pace might exacerbate pathological, addictive, or problem gambling behaviors.

With respect to each of these four categories of risks, we sought to answer three broad questions:

- (1) In the existing prohibitionist legal and regulatory regime, what level of protection are U.S. consumers afforded?
- (2) With legalization, could these risks be addressed more effectively than they are now, and assuming legalization, what regulatory strategy is best suited for addressing these risks?
- (3) What are the potentially relevant technologies and methods available for effective risk mitigation, and how might other parties contribute toward effective control?

Our answer to the threshold question of whether online gambling can be effectively regulated came out of our analysis of these more specific questions.

B. The Status Quo Offers No Effective Protection

Many U.S. residents already use online gambling services despite statutory restrictions. Recent estimates indicate that U.S. gamblers constitute roughly one-fourth to one-third of the global market for online gambling services.² The size of the U.S. share of that global market was estimated to be \$5.9 billion in 2008.³

The mainstay of the current prohibitionist regulatory structure is the Unlawful Internet Gambling Enforcement Act (UIGEA). Instead of criminalizing gambling itself, the UIGEA was intended to prevent U.S. residents from gambling by placing restrictions on the role of financial institutions in transmitting payments to and from gaming operators. However, because workarounds such as e-wallets (essentially a payment processor situated between banks and gambling sites), phone-based deposits, and prepaid credit cards have proliferated, very few U.S.-

² G. Srinivasan, "EU Slams US on Its Remote Gambling, Betting Laws," *Business Line*, June 14, 2009, <http://www.thehindubusinessline.com/2009/06/14/stories/2009061450870400.htm> (last accessed on September 10, 2009). Also noted in an August 4, 2009 interview with Simon Holliday, Director of H2 Gambling Capital (U.K.). Also see Simon Holliday *et al.*, *Internet Gambling Market Overview: AGA Internet Gaming Task Force*, H2 Gambling Capital, December 2, 2008, p. 8.

³ From H2 Gambling Capital, cited in American Gaming Association, *Internet Gambling*, AGA Fact Sheet, http://www.americangaming.org/Industry/factsheets/issues_detail.cfv?id=17 (last accessed on August 27, 2009).

based gamblers are presently much inconvenienced.⁴ Most gamblers are either unaware of or confused by the patchwork of federal and state restrictions, and many are readily guided by unregulated online gambling sites toward financial mechanisms that they can use to make deposits and withdrawals.⁵

The net effect is that the U.S. attempt to prohibit online gambling has instead pushed it offshore. Sites are readily available to U.S. residents through the essentially borderless medium of the Internet. Some sites are well-regulated, such as those based in the United Kingdom, Alderney, and Gibraltar, and others are less-well-regulated or unregulated, such as those in Antigua, Grenada, or the Kahnawake Mohawk territory. (Of course, it is the less-well-regulated international sites that provide easier access to U.S. consumers.) As a result of the global gaming industry's adaptations to the U.S. strategy, the United States finds itself in the unfortunate position of

- incurring all the social costs related to U.S. residents' online gambling;
- exercising no jurisdiction or control over the gaming sites that serve U.S. residents;
- being unable to offer U.S. residents who choose to gamble on overseas sites any consumer protections or to implement any other harm-reducing strategies; and
- being unable to qualify industry participants or even exclude criminal groups from competing for U.S.-based customers.

In an effort to address this reality and enforce current restrictions more aggressively, federal officials recently instructed four banks to freeze accounts belonging to online payment processors. The frozen accounts apparently contained funds owed to some 27,000 people who used offshore poker websites.⁶ Such financially based efforts seem to have had only a temporary chilling effect.⁷ Over the long run, it is probably not feasible for the federal government to prevent U.S. residents from accessing foreign sites via the Internet. Unlike China or Iran, for example, the United States has displayed no appetite for centralized control of the Internet to block citizens' access to undesirable sites.

⁴ USAplayers.com, *USA Poker Deposit Methods*, <http://www.usaplayers.com/poker/deposit-methods/index.html> (last accessed on August 8, 2009), and USAplayers.com, *Online Poker Deposits and the UIGEA*, <http://www.usaplayers.com/deposit-methods/articles/poker/online-poker-deposits-and-the-uigea.html> (last accessed on August 8, 2009).

⁵ Bo Bernhard *et al.*, *Internet Gambling in Nevada*, University of Nevada, Las Vegas, April 2007, at p. 26. Also see, Gilbert M. Gaul, "Players Gamble on Honesty, Security of Internet Betting," *The Washington Post*, November 30, 2008, p. A12.

⁶ Tamara Audi, "U.S. Deals Blow to Online-Poker Players," *The Wall Street Journal*, June 10, 2009, <http://online.wsj.com/article/SB124459561862800591.html> (last accessed on August 3, 2009).

⁷ Noted in an August 4, 2009 interview with Simon Holliday, Director of H2 Gambling Capital (U.K.).

Nor would criminalization of the gambling itself be an effective strategy.⁸ First, it would likely generate a massive pool of lawbreakers, almost none of whom would make attractive targets for criminal prosecution—because it would likely be a waste of law enforcement resources to pursue individual online gamblers. Second, it would exacerbate the dangers of consumer fraud at online gambling sites by making aggrieved consumers more reluctant to report their experiences.

C. Legalization and Regulation Would Afford Significantly Better Protection than the Status Quo

At a minimum, legalization and regulation of online gambling would give Americans much more protection than does the current prohibitionist regulatory framework. Although the kind of regulation that would accompany legalization would not be failsafe, it would be a significant improvement over the current regulatory and enforcement structure. We believe that safeguards could be implemented that would, on balance, substantially improve protections against the identified risks. These safeguards would also provide protection equal to or greater than that provided within the U.S.-based bricks-and-mortar gambling industry. We recognize that no set of technical or regulatory controls could ever eliminate these risks entirely. But even if the new fence had a few holes, it would be an improvement over having no fence at all.

The view that online gambling, in contrast to its bricks-and-mortar casino counterpart, is impossible to regulate reflects an old-fashioned perception of cyber jurisdictional authority. Many offshore commercial entities that operate online are subject to U.S. legal jurisdiction under existing long-arm statutes and authority. When coupled with governmental licensing authority, the ability to police online activities is even more powerful. Legalization with regulation would provide U.S. authorities with the power to grant or deny licenses and to impose significant sanctions on noncompliant licensees. Those licenses would be highly valuable to site operators. Compliance with any regulatory requirements and strict licensing conditions that Congress chooses to impose in return for the privilege of the license would therefore become a cost of doing business.

Just as with bricks-and-mortar casinos, the requirement for site operators to maintain a license gives the government the ability to exclude bad actors as well as impose a broad array of conditions for, and oversight of, licensees. In contrast, the current prohibitionist policy is extremely ineffective: large numbers of U.S. residents already gamble online, but they do so using offshore sites, many of which are poorly regulated.⁹ With legalization, we would expect

⁸ Ryan S. Landes, “Layovers and Cargo Ships: The Prohibition of Internet Gambling and a Proposed System of Regulation,” *New York University Law Review*, 82 (May 2007): 913–943, at p. 927–936. Also see Gerd Alexander, “The U.S. on Tilt: Why the Unlawful Internet Gambling Enforcement Act Is a Bad Bet,” *Duke Law & Technology Review*, No. 5 (2008), at ¶44. Also see Roger Clarke and Gillian Dempsey, “The Feasibility of Regulating Gambling on the Internet,” *Managerial and Decision Economics*, 22 (2001): 125–132, at p. 130. Also see Testimony of John Lyons, in U.S. House of Representatives, Committee on the Judiciary, *Establishing Consistent Enforcement Policies in the Context of Online Wagers*, 110th Cong., 1st Session, November 14, 2007, p. 107.

⁹ G. Srinivasan, “EU Slams US on Its Remote Gambling, Betting Laws,” *Business Line*, June 14, 2009, <http://www.thehindubusinessline.com/2009/06/14/stories/2009061450870400.htm> (last accessed on June 30, 2009). Also see *Supra* at footnote 6.

that most online gamblers would prefer licensed U.S.-based sites because of their integrity and security, rather than accept the risks posed by unregulated or poorly regulated sites. A well-structured regulatory regime would provide better protections against all of the risks we identified.

This conclusion is supported by the experience of other jurisdictions in regulating online gambling. Some of these, such as the United Kingdom and Alderney, have adopted regulatory regimes that appear to provide protection against the identified risks. That may be the most compelling evidence that online gambling can be effectively regulated.

D. Regulatory Methods and Technologies for Controlling Each Type of Risk Already Exist

For each of the 10 risks we examined, a set of regulatory methods and technologies already exists that would provide a reasonable degree of risk management. Moreover, most of them have been implemented in other countries. One general insight from regulatory policy, and a review of other country's experiences, is that no one size fits all: regulators should treat different risks differently. The incentives and motivations of different parties vary across risk categories, as does the locus for detection and control interventions. Understanding the natural incentives of the gaming industry with respect to each class of risk reveals whether a cooperative regulatory strategy would likely be more effective than a traditional enforcement-centric one.

For example, for at least one of the risks we identified (protecting the integrity of poker games by preventing players from colluding or conspiring to cheat other players), the interests of the public and of the gaming industry align reasonably closely. Both groups are interested in ensuring the integrity of the games. That makes a more cooperative and less adversarial regulatory relationship quite natural.

For other risks (such as defrauding of consumers by site operators, involvement of organized crime, and money laundering by site operators), a strict enforcement regime focused on identification and rapid exclusion of bad actors is more obviously appropriate. Oversight in these areas would focus heavily on up-front qualification or "suitability" to exclude those with criminal histories or connections and persons otherwise lacking in "good character, honesty, and integrity" as is the case in the bricks-and-mortar space. Enforcement activity would focus on bad actors, with the goal of exclusion and sanction. The intense and strict monitoring regime for reputable sites would include provisions designed to prevent or reveal any infiltration over time by undesirable groups or influences. Such regulations would mirror those now in place for bricks-and-mortar casinos.

Reputable sites, whose competitive advantage lies substantially with their reputation for integrity, would not be much troubled by the type of oversight designed to keep the "good character, honesty, and integrity" bar for admission high and the bad players out. In fact, they should appreciate such oversight as a positive contribution to the overall public perception of

their industry, and the regulatory certainty provided by a licensing model would help with the industry's overall long-term planning.¹⁰

Some risks (gambling by minors, money laundering by players, problem gambling, breaches of data confidentiality, and lack of site and technology security) present more complex challenges in terms of regulatory design. If site operators were driven solely by their short-run economic incentives, they would more likely take bets from minors, problem gamblers, and money launderers (because the sites gain financially, at least in the short run, from all such bets), and they might limit their investments in data privacy and security. Site operators might also gain, in the short run, from abusing or selling personal and financial data provided to them by gamblers.

In the longer term, of course, site operators value their brand names and reputations matter, and these five risks all figure as *reputational risks* from the industry's perspective just as they do in the bricks-and-mortar gambling industry. By setting the admission bar for licensees suitably high, U.S. regulators would intend to admit only reputable operators, whose behaviors would be guided by the value they place on establishing and maintaining a trusted brand. This is the approach taken by regulators in other jurisdictions—license only reputable firms. Probity investigations are conducted into the companies and their associates before a license is issued.¹¹ Hence, for these five risks, close supervision would be required if an operator were regarded as a rational but short-sighted actor. At the same time, a more cooperative and symbiotic regulatory relationship ought to emerge when reputable operators take a longer-term, strategic view. To better align site operators' short- and long-term interests, regulation also would provide for sanctions, from monetary fines up to and including loss of license for those site operators that choose to disregard mandated operational and consumer protections.

One strategy to provide longer-term, reputation-based incentives for good behavior is to create costs to entry—through the regulatory process, licensing fees, or other means—that reduce incentives to make a quick profit and leave the industry. For all risks created by operator shortsightedness, regulators need to establish and retain sufficient audit and monitoring systems so they can see when organizations that are otherwise reputable tilt too heavily toward short-term gain at the expense of public protection. Regulators should not accept the industry's protestations that they can be entirely trusted to take care of such risks without oversight simply because it is in their interest to do so. It is indeed in the industry's long-term interests to do so,

¹⁰ Noted in an August 13, 2009 correspondence with Katharina Riedl of bwin (Austria).

¹¹ Noted in an interview with Phill Brear, Head of Gambling Regulation at the Gibraltar Regulatory Authority and an interview with Glenn Gibson, Manager of Technical and Systems Audit at the Tasmanian Gaming Commission, and Damien Jarvis, Assistant Director of the Liquor and Gaming Branch of the Tasmania Department of Treasury and Finance (Australia). Also, as noted in an August 31, 2009 correspondence with John Sealy, Manager of Information Systems and Technology Services at the Licensing, Regulation and Alcohol Strategy Division of the Northern Territory Department of Justice (Australia), licensees often wish to be seen as responsible and as good corporate citizens. Also see Testimony of André Wilsenach and Testimony of Mary Williams, in U.S. House of Representatives, Committee on Financial Services, *Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?* 110th Cong., 1st Session, June 8, 2007, p. 122 and 140.

but short-term considerations sometimes prevail, even in major corporations and multibillion dollar industries.

The following sections of this study describe a variety of control technologies and regulatory tactics relevant to each risk, and identify the most promising approaches in each case. Table 1, in Appendix A, lists the 10 risks and for each outlines

- the level of protection afforded under the current regime (column 2);
- the overall structure and style of regulatory oversight most natural for each risk (column 3), and
- some key points regarding relevant technologies and control strategies (column 4).

Below we summarize key points in relation to each risk.

1. Gambling by Minors

There is a general concern that underage gamblers may access or attempt to access online gambling sites.

- Gambling by minors: A number of technologies routinely used in other industries can be used to exclude minors from online gambling, including a variety of data-matching techniques, electronic or other submission of documentary evidence of age, and possibly application of biometric identification systems. The strongest form of control would require positive matching of a player at the time of registration against existing databases of known adults, thus excluding minors, as well as identity-verification prior to initiating any session of play. U.S.-licensed operators would be expected to use filters and procedures that are as discriminating as reasonably possible. With respect to U.S. residents, we would expect available data needed for age-verification to be of high quality and reliability. Site operators could also be required to provide child-protective software to parents to help prevent minors from accessing gambling sites. Alternatively, a separate governmental or nonprofit entity could provide such software.

2. Criminal and Fraudulent Behavior

Criminal activity can stem from site operators or the players themselves. The following risks are related to criminal activity by site operators:

- Defrauding of consumers by site operators,
- Involvement of organized crime in gambling operations, and
- Money laundering by site operators.

These risks would be effectively limited by a regulatory strategy designed to keep the bar for admission high and to keep criminals out. Such controls have worked well in bricks-and-mortar casinos and would operate similarly with U.S.-licensed online site operators. Relevant tactics include rigorous vetting procedures for new applicants and monitoring of licensed site operator behavior to prevent or detect regulatory noncompliance, criminal conduct, fraudulent and deceptive practices, and disregard for consumers' rights.

Regulatory strategy with respect to these risks would be enforcement-centric with a focus on excluding operators with criminal histories or connections. Reputable site operators with brands to protect could not afford to risk damage to their reputations, loss of their licenses, or regulatory sanctions. Thus, we would expect the industry at large to support the type of demanding admission standards, regulatory monitoring, and sanctions designed to keep bad actors out of the business. Players, best positioned to detect improper conduct or consumer fraud by site operators, would be enabled and encouraged to report site operators' improper conduct directly to regulators and others in law enforcement. Players would also have access to U.S. courts for dispute resolution.

Player criminal behavior falls into two major categories—cheating or defrauding of players by other players and money laundering by players.

- Cheating or defrauding of players by other players: Most of the cases of improper player collusion or cheating that have come to light have been detected by other players. With a regulator in place for U.S.-licensed sites, players would have stronger recourse against the sites, or against other players, by lodging complaints with the regulator or relevant law enforcement agencies. More important, licensed operators could be required to maintain comprehensive databases of all betting transactions and these databases could be examined and analyzed by regulators in the event of an inquiry or the triggering of red flags. Site operators, who themselves have a strong interest in maintaining the integrity of their games, could be expected or even required to implement pattern recognition software to scan routinely for anomalous betting patterns.
- Money laundering by players: Online gambling operators, like operators of bricks-and-mortar casinos, would be subject to current anti-money-laundering regulations. These regulations would require site operators to expend some level of effort in detecting money laundering. The online environment provides *better* opportunities for detecting money laundering by players or player groups than the bricks-and-mortar casino environment. Site operators could be required to retain comprehensive data on all deposits, withdrawals, and betting transactions and to make these data available to regulators for examination and analysis. Given complete data, most patterns related to money laundering (such as light betting or matched bets placed by collaborators) would be easier to detect than they are in a physical environment (where complete transaction histories are available only in the form of video recordings). Software that detects anomalies and suspicious behaviors could be operated easily and routinely on digital databases by the site operators, by regulators, or by both. The site operators' obligations with respect

to their own detection of money laundering would form a part of their ordinary compliance obligations under the licensing regime.

3. Network Access, Data Privacy and Security Issues

Any U.S. legalization and regulatory regime would likely address the risk of access to online gambling sites from jurisdictions that prohibit such activity.

- Violation of jurisdictional restrictions or prohibitions: State, local, and tribal governments may continue to prohibit or restrict (1) the operation of gambling sites from within their jurisdictions and (2) online gambling by individuals resident or physically present within their jurisdiction. Licensed U.S. sites could be required to take all reasonable steps not to permit registration or participation by individuals in such states. A range of geolocation technologies are now available, mostly tied to identification of the user location by reference to their IP addresses. Such technologies, while not entirely foolproof, have the capability of reducing risks as much as is required by regulators. IP geolocation, together with address verification at registration and other controls, can be expected to deter the bulk of casual attempts to gamble from within restricted states. Determined users, of course, already have access to foreign sites and would probably continue to use those rather than go to the trouble of devising sophisticated technological means for defeating U.S.-based geolocation controls. Regulatory oversight methods could include audits of U.S.-based operators' software controls and routine "mystery shopping" at U.S. sites conducted from locations within states that had chosen to exercise their rights to restrict online gambling.

Data privacy and security risks include: sites not using commercially appropriate security systems and practices; intentional or accidental breach of the gambling site's and user's data security; and the introduction of spyware, adware, or malicious code into gambling websites' software or transmission of such malware to users' computers.

- Breaches of data confidentiality: Under legalization and regulation, U.S.-licensed operators would be subject to all applicable federal and state requirements regarding data confidentiality and security. Site operators would be subject to regulatory and potentially criminal sanctions and civil liability for any breaches or abuses of personal or financial data. Their data-protection controls would be subject to regulatory audit. There is no reason to believe that licensed online gambling operators would be any less able or willing to fulfill these obligations than other online merchants with similar data custody obligations.
- Communications and computer security failures: Under the current regime, U.S. authorities have no oversight over security for online gambling sites. With legalization and regulation U.S. licensed sites would be subject to existing data protection laws. Furthermore, U.S. regulators would have an opportunity to require state-of-the-art cybersecurity controls to protect against the introduction of malicious code or the unauthorized manipulation of games.

4. Problem Gambling

It is relatively easy to demonstrate for the other risk categories that a well-structured regulatory regime coupled with relevant technologies should provide better protection than the status quo. For problem gambling, however, the potential effect of legalization is less obvious a priori. Many might assume that pathological or addictive gambling behaviors would be exacerbated by the increased opportunity to gamble at any time and from anywhere online. But research on this topic does not support this conclusion. In particular, the link between the availability of online gambling and increases in the prevalence of problem gambling has not been established. Nevertheless, some online gamblers would be problem gamblers.

In a well-regulated online environment, gamblers could have opportunities and technologies made available to them to help curb addictive or problematic gambling behaviors. Such mechanisms would permit them to limit their gambling volume, deposit rates, loss rates, and the size of each wager. Users could also access online clinical and self-help resources from links provided at the gambling site.

The relationship between legalization and potential effects on problem gambling rates must certainly be examined carefully. Opponents of legalization fear an increase in problem gambling rates. However, gambling experts in the United States and the United Kingdom have reported that the prevalence rates for pathological gambling have remained static and low (roughly 0.7% of the adult population, in both countries) for many years. A large-scale study of gambling prevalence in the U.K. found the 0.7% rate remaining stable from 1999 through 2007 despite substantial increases in gambling opportunities during this period.¹²

Because this issue is likely to receive considerable attention as the United States considers legalization, we have attempted to analyze the various arguments given as to why the act of legalization might drive the level of problem gambling up or down. We have identified five popularly discussed mechanisms through which legalization could drive problem gambling *up*, and describe them here along with some observations that help mitigate the anticipated effects:

- Mechanism: Inhibitions to gamble that are based on would-be gamblers' knowledge of current legal restrictions would be removed.
- ❖ Observation: Gamblers in the United States are generally ignorant of or completely confused about existing legal restrictions, and (until very recently) there has been no enforcement against the gamblers

¹² Noted in a June 10, 2009 interview with Howard Shaffer, Director of the Division on Addictions and Associate Professor of Psychology in the Department of Psychiatry at the Cambridge Health Alliance. Also see Jacob Sullum, "Some Bets Are Off: The Strangely Selective and Self-defeating Crackdown on Internet Gambling," *reasononline*, June 2008, <http://www.reason.com/news/show/126022.html> (last accessed on September 10, 2009). Also see Heather Wardle *et al.*, *British Gambling Prevalence Survey 2007*, National Centre for Social Research, Prepared for the Gambling Commission, September 2007, <http://www.gamblingcommission.gov.uk/pdf/British%20Gambling%20Prevalence%20Survey%2007%20-%20Sept%202007.pdf> (last accessed on September 10, 2009), p. 10.

themselves.¹³ Hence, the lifting of the prohibition itself is unlikely to have any significant impact on would-be gamblers' willingness to gamble online.

- Mechanism: Gamblers may be more comfortable gambling online because licensed operators are reputed to be trustworthy.
 - ❖ Observation: The gamblers most likely to be influenced by the availability of trusted brand-name sites are those who gamble already, perhaps in the casino environment, and hence know the brands. Knowledgeable gamblers may indeed shift their business, but this represents displacement, not overall growth. And the displacement would be from bricks-and-mortar to online gambling, which can offer many more options and protections for problem gamblers than can land-based casinos.
- Mechanism: Gambling opportunities would be ubiquitous and available 24/7.
 - ❖ Observation: U.S. residents already have online gambling options available to them all day, everyday, and from anywhere. So the addition of U.S.-licensed sites would not alter that particular reality.
- Mechanism: Lifting the UIGEA's restrictions on financial transactions might make it easier for consumers to place bets online.
 - ❖ Observation: Lifting the restrictions of the UIGEA would not make it significantly easier for U.S. residents to make deposits to online sites. Enough workarounds have been designed, and are energetically promoted to consumers by the offshore sites, to render the existing restrictions largely ineffective.¹⁴
- Mechanism: Advertising by licensed online gambling sites might lead to increased problem gambling.
 - ❖ Observation: Although advertising is one avenue for the expected increase in online gambling that would follow legalization, little evidence exists to show whether and to what extent advertising-induced growth in, or redistribution of, gambling volume might produce increases in problem gambling rates.¹⁵ Furthermore, this mechanism (allowing advertising for

¹³ The recent seizure of online poker players' funds was termed an "unprecedented action" by the Poker Players Alliance. See *Supra* at footnote 6.

¹⁴ See *Supra* at footnote 4.

¹⁵ Noted in an August 4, 2009 interview with Simon Holliday, Director of H2 Gambling Capital (U.K.).

online gambling sites) is controllable to the extent deemed necessary or desirable, through regulatory restriction.

We also looked at two mechanisms through which legalization and regulation could drive problem gambling *down*:

- Mechanism: Tax and license-fee revenue distributions may provide an opportunity to extend and enhance counseling, treatment, and support programs for problem gamblers.
 - ❖ Observation: Significant tax revenues might be anticipated from U.S. operators, and revenue distributions from taxes and license fees could substantially boost publicly funded prevention, counseling, and treatment programs, as well as research on gambling addiction. Existing budgets for counseling and treatment services for problem gamblers have been limited, and most health insurance programs do not currently cover these services.¹⁶
- Mechanism: Regulators could require licensed domestic sites to lead the world in offering a full suite of advice and protections for problem gamblers to an even greater extent than is the case in bricks-and-mortar casinos.
 - ❖ Observation: U.S.-licensed sites could be required to display offers of help prominently on their websites, including (1) registration pages that offer self-diagnostic tests designed to help would-be gamblers understand their own attitudes and vulnerabilities; (2) web pages that display prominent links to support and counseling services; and (3) availability of speed-of-play, compulsory time-outs, or player-loss-rate caps. All players should be offered the opportunity up front and at subsequent intervals to voluntarily exclude themselves or to limit their own deposit rates, loss rates, betting rates, or periods of play.

We believe that the opportunities to mitigate problem gambling provide significant benefits not available under the status quo. These benefits provide a significant counterweight to any potential increases in problem gambling that result from legalization. Furthermore, the potential benefits of mitigation would become available to most existing online problem gamblers.\

¹⁶ Franklin (2001) discusses lack of federal funding for treatment or awareness of problem gambling, lack of insurance parity for problem gamblers, and limited or lack of funding from most states in the United States. Joanna Franklin, *Problem Gambling in the U.S: From the Beginning – Into 2001*, http://www.responsiblegambling.org/articles/Problem_and_Pathological_Gambling_A_view_from_the_States.pdf (last accessed on September 10, 2009). Also, Winslow (2008) discusses the lack of state funding for problem gambling services in Colorado and other states in the United States. Kyle Winslow, “A Problem for Gamblers,” *The American Prospect*, March 10, 2008, http://www.prospect.org/cs/articles?article=a_problem_for_gamblers (last accessed on July 13, 2009). Also see the website of the Association of Problem Gambling Service Administrators (APGSA), <http://www.apgsa.org/State/index.aspx> (last accessed on September 10, 2009).

E. Conclusions

We have examined 10 distinct risks in four categories that may be associated with the growth and availability of online gambling. In each case, the current legislative framework is failing to provide any effective risk control or consumer protection. The establishment of a well-regulated industry under U.S. jurisdiction would offer the opportunity for much better protection. We recommend that plans for regulating online gambling include the design and use of different risk-control strategies for different risks that may be associated with Internet gambling, as well as education and consumer support.

If the United States decides to legalize and regulate online gambling sites, we would expect most U.S.-resident gamblers to be diverted from overseas sites toward reputable and trusted domestic operators. In the long run, reputable gambling operations under U.S. control should come to dominate online gambling opportunities chosen by U.S. consumers. All four categories of risk would be better controlled in such circumstances than they are at present. In the end, U.S. consumers would be better protected than they are now.

II. REGULATORY METHODS AND TECHNOLOGIES AVAILABLE FOR CONTROLLING EACH RISK

For each of the 10 risks outlined above, a set of regulatory methods and technologies already exists that would provide a reasonable degree of control. Moreover, most of them have been implemented successfully in other countries and other online settings. This section describes a variety of control technologies and regulatory tactics relevant to each risk, and identifies the most promising approaches in each case.

A. Gambling by Minors

A common concern about legalizing online gambling stems from the fact that many current online gambling sites do not have adequate regulations or safeguards against gambling by minors. The primary concern is that underage access to and use of online gambling services might increase because it may be difficult to verify age and replicate controls used by bricks-and-mortar casinos to exclude minors. However, effective measures to prevent online gambling by minors have been implemented in well-regulated Internet gambling environments in many European countries and in Australia. Moreover, a number of technologies routinely used in other industries can be applied to the online gambling environment. We discuss below the issue of online gambling by minors and strategies to prevent it.

1. The Issue of Gambling by Minors

Age restrictions apply to virtually all forms of legalized gambling, though the specific age restriction varies by jurisdiction. The typical rationale for age restrictions is that children and young persons are highly vulnerable and are more likely to become problem gamblers if they begin gambling at a young age. In the online environment, gambling by minors is a problem that stems from the inherent difficulty in separating underage users from adults on the Internet because of the absence of an official personally verifying a gambler's age.¹⁷ Minors can gain access to online gambling websites either by providing false credentials during the registration process or by gaining access to their parents' or others' online gambling account.

Anecdotal evidence suggests and surveys have shown that underage gambling is widespread. Studies conducted between 1999 and 2004 covering Canada, the United States, the United Kingdom, and Australia indicated that 4–7% of adolescents exhibited serious patterns of pathological gambling and 10–15% were at risk of either developing or returning to a serious gambling problem.¹⁸ More recent studies have revealed an increase in the involvement of

¹⁷ Ryan S. Landes, "Layovers and Cargo Ships: The Prohibition of Internet Gambling and a Proposed System of Regulation," *New York University Law Review*, 82 (May 2007): 913–943 at p. 923.

¹⁸ Sally Monaghan, *Internet and Wireless Gambling – A Current Profile*, Australasian Gaming Council, 2008. http://www.austgamingcouncil.org.au/images/pdf/Discussion_Papers/agc_dis_internet.pdf (last accessed on July 11, 2009). Also the extent to which rates of problem gambling among adolescents are elevated is controversial. For example, in exploring the properties of two screening instruments in identifying problem gambling among students aged 15 to 17, Ladouceur *et al.* (2005) discuss the need to clarify the construct of pathological gambling among youth and note that neither the SOGS nor the DSM-IV subscale (MAGS) was perfect in identifying problem gambling. R Ladouceur *et al.*, "Concordance between the SOGS-RA and the

(continued...)

Canadian youth in online gambling. In 2006, 9% of Canadian high school students reported having gambled online for money, an increase from 3.6% in 2005.¹⁹ According to the National Annenberg Survey of Youth, in the United States, card playing for money on the Internet by male youth aged 14 to 22 rose to 3.3% in 2008 from 2.4% in 2007.²⁰ In a 2008 study of general gambling attitudes among Canadian youth aged eight to 20, 76% of those surveyed admitted to having gambled at least once in their lives.²¹ Among the group aged 18 to 20, 90% had gambled at least once and approximately 39% admitted to gambling once a week or more.²²

2. Existing Controls in Other Jurisdictions

States with commercial casino gambling typically limit access to persons 21 or over, although most lotteries and some Native American casinos allow 18-year-olds to gamble. Most other countries have an age limit of 18, which applies to both online and casino gambling. There is no established minimum age for online gambling in the United States because it is done outside of U.S. legal and regulatory safeguards.

Well-regulated overseas gambling jurisdictions require online operators to verify the identity, location, and age of their customers and to use various mechanisms to curb underage gambling. Some evidence suggests that age restrictions for online gambling have not been uniformly required or rigorously implemented. In an exploratory study of 30 U.K.-based sites conducted before the United Kingdom's regulation of online gambling, researchers noted that 11 of those sites had no age verification check.^{23, 24} Although 17 sites had age checks, they simply required a person registering to either check a box to confirm that they were 18 years of age or older or

DSM-IV Criteria for Pathological Gambling among Youth.” *Psychology of Addictive Behaviors*, 19, No. 3 (2005): 271–276 at p. 274-275.

¹⁹ J. McBride, “Internet Gambling among Youth: A Preliminary Examination,” *International Center for Youth Gambling Problems & High-Risk Behaviors Newsletter*, 6, No. 1 (2006); cited in Sally Monaghan, *Internet and Wireless Gambling – A Current Profile*, Australasian Gaming Council, 2008.

http://www.austgamingcouncil.org.au/images/pdf/Discussion_Papers/agc_dis_internet.pdf (last accessed July 11, 2009).

²⁰ The Annenberg Public Policy Center *Internet Gambling Stays Low Among Youth Ages 14 to 22 but Access to Gambling Sites Continues; Sports Gambling Makes Resurgence*, November 26, 2008, <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=306> (last accessed July 25, 2009).

²¹ Jeffrey L. Derevensky *et al.*, “Adolescent Attitudes toward Gambling,” *Brazilian Journal of Cognitive Psychology*, 4, No. 1 (2008), http://pepsic.bvs-psi.org.br/scielo.php?script=sci_arttext&pid=S1808-56872008000100002&lng=en&nrm= (last accessed on September 1, 2009).

²² See *Id.*

²³ U.K.-based online gambling operators first came under regulation with the introduction of the Gambling Act 2005 in September 2007. Before the Gambling Act, online gambling fell under no specific regulation.

²⁴ Michael Smeaton and Mark Griffiths, “Internet Gambling and Social Responsibility: An Exploratory Study,” *CyberPsychology & Behavior*, 7, No. 1 (2004): 49–57.

enter their date of birth.²⁵ In addition to lax age checks, most websites required only a valid credit card to begin gambling. However, some minors in the United States as young as 13 have access to credit cards in their name, rendering this mechanism ineffective as an age check.²⁶ Moreover, minors may have access to their parents' credit card information. In a 2004 British study, a 16-year-old girl attempted to access 37 gambling websites using her debit card, lying about her age but being otherwise truthful. Only seven sites prevented her from registering.²⁷

A more recent mystery shopping study performed between April 2008 and March 2009, after U.K.-based online gambling had come under regulation, revealed quite different results. The British Gambling Commission noted that more than 95% of gamblers were registered with websites that had sufficient age verification checks, and only 2.2% were registered with sites that had age verification weaknesses.²⁸

Other jurisdictions have also had success in preventing underage gambling through effective use of restrictions and mechanisms. In his testimony to Congress, the CEO of the Alderney Gambling Commission noted that during the seven years of regulation of online gambling in Alderney, the Commission had not had any complaints about minors gaining access to an Alderney-regulated site. He further noted that the primary reason that Alderney's licensed sites are able to prevent minors from gaining access is the use of third-party verification software by most licensees.²⁹

Similarly, Mary Williams of the Gambling Control Commission of the Isle of Man noted that license holders of online gambling websites use various methods of age verification, including large data services such as Experian, to ensure that customers are of legal age. Moreover,

²⁵ See *Id.*

²⁶ Commission on Child Online Protection, *Report to Congress*, October 20, 2000, <http://www.copacommission.org/report/COPAreport.pdf> (last accessed on August 11, 2009), p. 25. Also see European Commission, *Background Report on Cross Media Rating and Classification, and Age Verification Solutions*, Safer Internet Forum, September 2008, http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/reportageverification.pdf (last accessed on August 24, 2009).

²⁷ Smeaton *et al.*, "Study into Underage Access to Online Gambling and Betting Sites," 2004; cited in Ryan S. Landes, "Layovers and Cargo Ships: The Prohibition of Internet Gambling and a Proposed System of Regulation," *New York University Law Review*, 82 (2007), at p. 924.

²⁸ British Gambling Commission, *Online Mystery Shopping Programme*, July 2009, <http://www.gamblingcommission.gov.uk/pdf/online%20mystery%20shopping%20programme%20july%202009.pdf> (last accessed on August 2, 2009).

²⁹ Testimony of André Wilsenach, in U.S. House of Representatives, Committee on Financial Services, *Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?* 110th Cong., 1st Session, June 8, 2007, at p. 145.

withdrawal of funds requires access to a PIN number, which the gambling site mails to the user's postal address, thereby limiting the possibility of unauthorized access to funds by minors.³⁰

Gibraltar's regulatory regime requires licensees to take "all reasonable steps" to verify that customers are of legal age, although operators are allowed to consider the use of a credit card as a verification of age.³¹

The United Kingdom requires that licensed gambling sites have policies and procedures to prevent underage gambling, including a warning that underage gambling is illegal, requiring an affirmation from the customer that he or she is of legal age, ensuring that staff are trained in age verification (particularly in the use of secondary forms of identification verified by staff members when initial automated procedures fail), and enabling filtering software to block the website.³² Beyond this, secondary verification may be required, such as searching credit databases for age information, prohibiting unverified users from withdrawing winnings, and freezing the account of anyone not verified within 72 hours of applying to the site. However, these checks are not required if the user deposits funds using a credit card.³³

The regulator in Australia's Northern Territory requires that players' ages be confirmed within 90 days of opening an online gambling account and before withdrawing any funds. Copies of identification must be e-mailed, faxed, or mailed directly to the site operator. If the individual is not confirmed within the 90-day period, he or she must seek permission from the regulator's Director of Licensing to re-open the account.³⁴

In the United States, the UIGEA exempts certain forms of gambling, such as horse racing and state lotteries, from its criminal provisions if the applicable state law has a provision for age verification that is "reasonably designed to block access to minors."³⁵

³⁰ Testimony of Mary Williams, in U.S. House of Representatives, Committee on Financial Services, *Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?* 110th Cong., 1st Session, June 8, 2007, at p. 130.

³¹ Gibraltar Regulatory Authority, *Code of Practice for the Gambling Industry*, Issued by the Gambling Commissioner, December 13, 2008, http://www.gra.gi/sites/gambling/downloads/215/generic_code_v1.0.2009.pdf (last accessed on August 6, 2009), p. 14.

³² British Gambling Commission, *Conditions and Codes of Practice applicable to: Remote Casino Licenses, Remote Casino Ancillary Licenses*, December 2008, at p. 7–8.

³³ See *Id.*

³⁴ Noted in an August 31, 2009 correspondence with John Sealy, Manager of Information Systems and Technology Services at the Licensing, Regulation and Alcohol Strategy division of the Northern Territory Department of Justice (Australia).

³⁵ Anthony Cabot and John Aristotle Phillips, "Age Verification: UIGEA Compliance and Regulation," *World Online Gambling Law Report*, October 2006, <http://integrity.aristotle.com/documents/AgeVerificationLawPublication.pdf> (last accessed on August 10, 2009).

3. Relevant Technologies for Risk Mitigation

Although the anonymous nature of online platforms might increase the risk of underage gambling, available technologies can address such risks.

Researchers have outlined several categories of technologies for verifying the age of adults, including comparison of the registrant's credentials against public databases such as credit reports and criminal histories, or even biometrics.³⁶ In designing such controls, care would be needed to balance the (intended) exclusion of minors against the (unintended) denial of admission to qualified adults. The use of a credit card can often be an indicator of age, although, as noted in Section 2, some children have access to credit cards, and credit card companies do not allow cards to be used for age verification.³⁷ It is thus likely that any age verification technology would use government-issued identification as its basis, potentially combined with other strategies to increase its effectiveness.³⁸

Exclusion of minors from online gambling can also be aided through technologies routinely used to verify age in other applications today.³⁹ Currently, online liquor stores employ various mechanisms, including a variety of data-matching techniques, to prevent minors from purchasing alcohol online.⁴⁰ The simplest solution requires a social security number and other forms of identification such as a driver's license, combined with a credit card registered to that individual.⁴¹ An age-verification service is used to check the information provided against a database containing credit data, driver's license data, and registered voter information.⁴²

³⁶ Internet Safety Technical Task Force, *Enhancing Child Safety and Online Technologies*, Final Report to the Multi-State Working Group on Social Networking of State Attorneys, Berkman Center for Internet & Society, Harvard University, December 31, 2008, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf (last accessed on September 11, 2009) at p. 8.

³⁷ See *Supra* at footnote 35.

³⁸ See *Id.*

³⁹ Such as online liquor stores, online sellers of tobacco, and the websites of Hollywood movie studios. See Testimony of Michael Colopy, in U.S. House of Representatives, Committee on the Judiciary, *Establishing Consistent Enforcement Policies in the Context of Online Wagers*, 110th Cong., 1st Session, November 14, 2007, at p. 53.

⁴⁰ Boris Reznikov, "Can I See Some ID? Age Verification Requirements for the Online Liquor Store," *Shidler Journal for Law, Commerce & Technology* 4, No. 5 (2007), <http://www.lctjournal.washington.edu/Vol4/a05Reznikov.html> (last accessed on July 25, 2009). Also see Integrity, *Case Study: Age Verification for Online Alcohol Sales*, Aristotle Inc., http://integrity.aristotle.com/documents/Online_Wine_Sales-WhitePaper2006.pdf (last accessed on September 10, 2009).

⁴¹ See *Id.*

⁴² Noted in an August 5, 2009 interview with Phill Brear, Head of Gambling Regulation at the Gibraltar Regulatory Authority.

Aristotle, Inc., a technology consulting firm, produces an identity- and age-verification service called Integrity:Direct, which uses a database of government-issued identification to verify age; the vendor claims the check takes less than 5 seconds, covers 3.4 billion people, complies with U.S. privacy laws, and is not subject to the Fair Credit Reporting Act because it does not use any credit data.⁴³

LexisNexis and its advanced linking technology combines real time access to billions of public records compiled from thousands of public and proprietary sources that can be used to verify age and identity of individuals.⁴⁴ For a minor to defeat this method of authentication, he or she would have to access an adult's government-issued ID card, credit card, and other information. Because this is a foreseeable scenario, this age verification technique must be combined with others.

Michigan's Liquor Control Commission has approved a "knowledge based authentication" tool for age verification. This online tool develops questions that only the specific individual would know answers to and checks the answers against public records.⁴⁵ This system, while robust, imposes potentially significant transaction costs of between 25 cents and one dollar per check, making it a costly solution if used every time a user logs on to a gambling site.⁴⁶ The LexisNexis service can deliver an interactive, knowledge-based query process to instantly "multifactor" authenticate individuals at the point of customer contact.⁴⁷

Other technologies may prove useful to augment traditional verification, such as the use of a PIN number mailed to the address of record of the user, as in the Isle of Man, or requiring the user to enter personal information via his or her home phone. This strategy prevents a minor from simply using his or her parents' credit and ID cards and immediately creating an account.

If legalization is implemented and matching techniques are used, the U.S.-licensed site operators would be expected to develop and use filters that are discriminating. Regulators could choose where to set the balance between Type I errors (where underage gamblers are not detected) and Type II errors (where gamblers of legal age are excluded). Moreover, with respect to U.S.

⁴³ Integrity, *Integrity:Direct*, Aristotle Inc., http://integrity.aristotle.com/index2.php?option=com_content&do_pdf=1&id=47 (last accessed on August 11, 2009).

⁴⁴ Noted in an August 10, 2009 interview with Chris Pinion, National Account Manager at LexisNexis Risk and Information Analytics.

⁴⁵ See *Supra* at footnote 40. Also see Tricia Pearson, 'Can I See Some ID?' *Why Age Verification Is a Hot Topic for Online Retailers*, Shoosmiths, June 24, 2009, <http://www.shoosmiths.co.uk/news/2372.asp> (last accessed on August 11, 2009).

⁴⁶ See *Supra* at footnote 40 Boris Reznikov.

⁴⁷ Noted in an August 10, 2009 interview with Chris Pinion, National Account Manager at LexisNexis Risk and Information Analytics.

residents, we would expect available data to be of high quality and reliability, making age verification through matching techniques effective.⁴⁸

Site operators could also be required to provide child-protective software to parents to keep minors from accessing their parents' accounts or any online gambling sites. The Nova Scotia Gaming Corporation (NSGC) commissioned and distributed BetStopper, which is a software program designed to help parents prevent children from visiting online gambling websites. Results from the pilot survey were extremely positive and indicated that 92% of parents found BetStopper to be a valuable prevention tool.⁴⁹ The BetStopper software was provided to families for free by the NSGC. Other widely available Web filtering software, such as Net Nanny, can also be used to block access to gambling sites by children. Net Nanny analyzes keywords and objects on every website visited and assigns "points" in different content categories, one of which is gambling.⁵⁰ If a site scores too high in an objectionable category, the software blocks it.⁵¹ An administrator, usually a parent, can decide which categories to block and also whether a particular score leads simply to a warning message or to a complete block.⁵² The software has generally received high reviews, and its filtering technology is resistant to circumvention.⁵³ Other parental control tools are contained within operating systems such as Windows Vista and Mac OS X, some are provided for free by network service providers, and many online safety organizations provide directories to help parents find appropriate protective software.⁵⁴ A regulator may require that approved filtering software be offered to anyone requesting it.

Minors may also have a weak financial motive to gamble online. If a minor usurps an adult's payment and identification information, for example, all of the minor's winnings would be paid

⁴⁸ Noted in an August 5, 2009 interview with Phill Brear, Head of Gambling Regulation at the Gibraltar Regulatory Authority. Also noted in an August 21, 2009 interview with Andrew Fritchie, General Counsel of PartyGaming PLC.

⁴⁹ Nova Scotia Gaming Corporation, World-Leading Software Launched to Protect Nova Scotia Youth, May 29, 2009, <http://www.nsgc.ca/pdf/press/Microsoft%20Word%20%20BetStopper%20Media%20Release%20FINALMay%2028%20w%20photo.pdf> (last accessed on September 10, 2009).

⁵⁰ Net Nanny, Protecting Your Family on the Internet, white paper, http://www.netnanny.com/products/netnanny/protecting_your_family (last accessed on September 10, 2009).

⁵¹ See *Id.*

⁵² See *Id.*

⁵³ For a review of the Net Nanny software, see <http://internet-filter-review.toptenreviews.com/netnanny-review-pg2.html> (last accessed on September 10, 2009).

⁵⁴ Federal Communications Commission, Report in the Matter of Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming, MB Docket No. 09-26, released August 31, 2009, at ¶142, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-69A1.pdf (last accessed on September 1, 2009).

directly to the adult's account.⁵⁵ For a minor to benefit financially from gambling, he or she would have to have access to his or her own payment mechanism, such as a credit card or bank account, but the demographic information associated with the account would more easily allow the website to verify the user's age. Similarly, the regulator could require forfeiture to the government of winnings to gamblers who are discovered to be underage, further lowering the financial incentive for minors to gamble online.⁵⁶

Regulators could impose harsh penalties on site operators with lax mechanisms to prevent underage gambling. Frequent and widespread mystery shopping, as done in the United Kingdom, can reveal operators with inadequate safeguards in place to curb underage gambling. The regulator can impose penalties on such operators, including monetary fines, the revocation of the gambling license, and even criminal liability.

Moreover, to help combat underage gambling, a portion of online gambling tax revenues could be earmarked for educational programs for parents and minors. Given sufficient funds, a regulator may require that youth gambling prevention lessons be incorporated into school curricula. In South Australia, the "Don't Bet On It!" program was introduced as a way to educate children about the dangers of youth gambling. A 2002 report claimed a "small but statistically significant change in student attitudes towards gambling" as a result of the curriculum, which includes five lessons, a mock gambling game, and pre- and postactivity surveys.⁵⁷ The report also describes other educational programs from entities in Australia and in North America, such as the Minnesota Institute of Public Health and Saskatchewan Health in Canada.⁵⁸

4. Conclusion

The current state of affairs, with U.S. residents accessing online gambling sites with widely varying degrees of regulation, does not provide comprehensive protections to ensure that gamblers are of legal age. Regulatory mechanisms and technological solutions, many of which are currently used in other jurisdictions and industries, can equip online gambling operators with capabilities to selectively exclude minors from engaging in online gambling. Age verification policies would be less effective in the absence of support from minors' parents and guardians; therefore, a successful regulatory strategy would provide tools with which parents can limit

⁵⁵ Jonathan Gottfried, "The Federal Framework for Internet Gambling," *Richmond Journal of Law & Technology*, X, No. 3, at p. 10, <http://law.richmond.edu/jolt/v10i3/article26.pdf> (last accessed on August 6, 2009).

⁵⁶ Noted in an August 5, 2009 interview with Glenn Gibson, Manager of Technical and Systems Audit at the Tasmanian Gaming Commission, and Damien Jarvis, Assistant Director of the Liquor and Gaming Branch of the Tasmania Department of Treasury and Finance (Australia).

⁵⁷ Loris Glass, *Gambling Education: Some Strategies for South Australian Schools*, funded by the Gamblers Rehabilitation Fund, South Australia, November 2002, at p. 19–20, <https://www.library.health.sa.gov.au/Portals/0/gambling-education-some-strategies-for-south-australian-schools.pdf> (last accessed on September 10, 2009).

⁵⁸ See *Id.* at p. 20–22.

access to gambling websites by their children. We believe that online gambling can effectively exclude minors when it combines cutting-edge technology with a strong regulatory regime.

B. Defrauding of Consumers by Site Operators

Gambling websites, which deal with large amounts of money in a virtual setting, have the potential for fraudulent activity and unfair dealings.⁵⁹ As discussed below, unregulated gambling sites have been known to defraud customers and steal significant sums of money.⁶⁰ However, a system of effective regulation could manage the risks of fraud and ensure fair and legal dealings.

1. The Issue of Fraud by Site Operators

Fraud by site operators can be classified into three broad categories:

- Individuals can set up unlicensed gambling websites that either refuse to return customers' deposits or operate unfair games.
- Operators can model a fraudulent website after a licensed site and siphon players from the more reputable operator.
- Insiders within reputable websites can exploit inside information to cheat players without the knowledge of the larger organization.

It is reasonably easy for an individual to set up a fraudulent site, attract as many depositors as possible, and then either shut down the site and take the deposits or continue to run the site with odds or fees swung decidedly in the operator's favor. As a site's reputation became tarnished, it would quickly lose its base of players, but it could then simply shut down and open a new site, perpetrating the same fraud over and over again.⁶¹ The identity of site owners is often unclear, and the ease of transferring between sites makes this method of fraud highly profitable.⁶²

Reputation is clearly a major attribute of gambling websites. Websites can piggyback on, or usurp, the reputation of a reputable operator or jurisdiction to instill confidence in consumers. For instance, "Casino Australia (<http://www.casinoaustralia.com/>) is an attractive site emblazoned with images of Sydney, koalas, and the national flag but has no other connection with Australia. The online casino is physically located in the Netherlands Antilles and marketed

⁵⁹ Gerd Alexander, "The U.S. on Tilt: Why the Unlawful Internet Gambling Enforcement Act is a Bad Bet," *Duke Law & Technology Review*, 5 (2008), at ¶9.

⁶⁰ See, for example, Financial Crimes Enforcement Network, *A Survey of Electronic Cash, Electronic Banking, and Internet Gaming*, U.S. Department of the Treasury, 2000, at p. 41; and see *Supra* at footnote 17 at p. 925.

⁶¹ See *Supra* at footnote 17, at page 925.

⁶² See *Id.*

by a Native American gambling corporation.”⁶³ Because gambling websites are often based in countries far from their target customers, they can often avoid legal accountability, and because website creation is relatively simple, a customer can be easily confused about the licenses and controls held by a particular site.⁶⁴

In addition to fraud by gambling sites themselves, employees or executives of sites may initiate fraud at the individual level without the knowledge of the organization as a whole. In September 2007, players at the poker website Absolute Poker initiated their own investigation into apparent cheating by a player in a tournament. The investigation revealed that a co-owner of the company and a former director of operations had acted in concert to cheat players of amounts between \$500,000 and \$1 million.⁶⁵ Another poker website, UltimateBet, was rocked by a cheating scandal in early 2008 triggered by concerns about one online player who could apparently see other players’ hole cards during play. Investigation revealed that from January 2005 to December 2007, former employees of the company, operating from outside, had exploited security vulnerabilities in the site’s software of which only they were aware.⁶⁶

Since the enactment of the UIGEA, U.S. residents no longer have access to large gambling sites operated by publicly-traded companies; instead, U.S. gamblers look to less transparent offshore site operators that may be more likely to engage in fraud or other deceitful practices.⁶⁷ Also, given the current absence of regulatory oversight in the United States, U.S. gamblers have little or no recourse to authorities when site operators defraud them.⁶⁸

The extent of fraud by site operators is not well documented, but cases have been recorded. A 2000 report by the Financial Crimes Enforcement Network of the U.S. Department of the Treasury claims that “[t]here is, in fact, a substantial record of shadow websites collecting...deposits for a period of time and then disappearing, in the process destroying

⁶³ Roger Clarke and Gillian Dempsey, “The Feasibility of Regulating Gambling on the Internet,” *Managerial and Decision Economics*, 22 (2001): 125–132, at p. 128.

⁶⁴ See *Id.*

⁶⁵ Russell Goldman, “Online Poker Players Expose Alleged Fraud,” *ABC News*, October 19, 2007. <http://abcnews.go.com/print?id=3752500> (last accessed on July 24, 2009)

⁶⁶ UltimateBet.com, *UltimateBet Issues Statement Regarding Unfair Play*, May 29, 2008. <http://www.ultimatebet.com/poker-news/2008/may/NioNio-Findings> (last accessed on July 24, 2009). Also see UltimateBet.com, *Status Update on NioNio Investigation*, July 8, 2008, <http://www.ultimatebet.com/poker-news/2008/july/Investigation-Status-Update> (last accessed on July 24, 2009).

⁶⁷ As noted in an August 21, 2009 interview with Andrew Fritchie, General Counsel of PartyGaming PLC, U.S. customers are forced to use privately-held sites, which are generally perceived as less reputable.

⁶⁸ See *Supra* at footnote 17 at p. 926. Also see *Supra* at footnote 59 at ¶¶14–15. Also see Christopher Grohman, “Reconsidering Regulation: A Historical View of the Legality of Internet Poker and Discussion of the Internet Gambling Ban of 2006,” *Journal of Legal Technology Risk Management*, 1, No. 1 (Fall 2006): 34–74, at p. 62–63.

consumer confidence.”⁶⁹ In a 2006 survey, the American Gaming Association reported that 55% of respondents “agree[d] at least somewhat that online casinos find ways to cheat players.”⁷⁰ The website *GamesandCasino.com* maintains and publishes a long “blacklist” of websites that cheat, defraud, or otherwise manipulate their users.⁷¹ Finally, in a 2007 survey of Nevadans conducted by the International Gaming Institute at the University of Nevada, Las Vegas (UNLV), 66.9% of respondents (who were not necessarily gamblers) claimed to have “strong doubts about the integrity of online gambling as it pertain[s] to the ability to cheat the gambler.”⁷² The survey also includes various anecdotes from respondents about cheating by site operators.⁷³

In addition to outright fraud by site operators, operators may become bankrupt or otherwise insolvent without engaging in questionable business practices. Without adequate financial protection, customers could lose their entire fund balance with the site.⁷⁴ As shown below, existing controls such as holding customers’ funds in a trust account or establishing financial reserves can help mitigate against this business risk to customers.

2. Existing Controls in Other Jurisdictions

Most regulatory regimes address the issue of operator fraud. In the United States, a regulatory strategy could combine elements from other regimes and add unique safeguards. Below are descriptions of approaches taken to prevent operator fraud in other jurisdictions:

- The Gambling Control Commission of Alderney, a Channel Island, requires sites to have “provisions enabling the customer to address complaints and disputes to an independent body.”⁷⁵
- In the Isle of Man, site operators are required to maintain either financial reserves or a bond to ensure that players are paid their winnings.⁷⁶

⁶⁹ Financial Crimes Enforcement Network, *A Survey of Electronic Cash, Electronic Banking, and Internet Gaming*, U.S. Department of the Treasury, 2000, at p. 41.

⁷⁰ American Gaming Association, *State of the States: The AGA Survey of Casino Entertainment*, 2006, at p. 21, http://www.americangaming.org/assets/files/2006_Survey_for_Web.pdf (last accessed on July 23, 2009)

⁷¹ GamesandCasino.com, *Blacklisted Casinos*, <http://www.gamesandcasino.com/blacklist.htm> (last accessed on September 10, 2009).

⁷² See *Supra* at footnote 5 Bo Bernhard at p. 37–38.

⁷³ See *Id.* at p. 40–43.

⁷⁴ Noted in an August 27, 2009 interview with André Wilsenach, Chief Executive Officer of the Alderney Gambling Control Commission.

⁷⁵ See *Supra* at footnote 29 at p. 142–143.

⁷⁶ See *Supra* at footnote 30 at p. 124.

- Antigua’s and Barbuda’s regulations require a site operator to maintain “investments that have a market value...of not less than the aggregate amount of all its outstanding prizes and monies held on account for players.”⁷⁷
- The British Gambling Commission sets forth rules governing licensed gambling website operators, including one that requires that licensees (1) inform customers as to whether their funds are protected in the event of insolvency and (2) “be able to provide evidence to the [U.K. Gambling] Commission, if required, showing how they satisfied themselves that their terms are not unfair.”⁷⁸ The U.K. Department of Culture, Media and Sport (the sponsor of the Gambling Commission) publishes the “White List,” a list of nations hosting online gambling whose licensees are legally permitted to advertise in the U.K, although the list is currently in a state of suspension.⁷⁹
- Tasmania’s regulator sets technical standards and uses independent accredited testers to verify compliance before approving new software, and for some types of operations also requires that players funds be held in a trust for the protection of players.⁸⁰
- Gibraltar’s regulator requires licensees to have strong internal controls and also requires independent testing of gambling software to ensure integrity.⁸¹

Although the regulatory schemes described above include provisions to prevent fraud, effective regulation must include strong penalties for noncompliance and safeguards that protect customers in the event of fraud or wrongdoing. They also should mandate ordinary but rigorous due diligence by regulators and owners, including background checks on owners, operators, and

⁷⁷ Antigua and Barbuda – Directorate of Offshore Gaming, “Interactive Gaming and Interactive Wagering Regulations,” at §184(a).
http://www.antiguagaming.gov.ag/files/Antigua_and_Barbuda_Gaming_Regulations-Final.pdf
 (last accessed July 23, 2009)

⁷⁸ See *Supra* at footnote 32 at p. 14.

⁷⁹ Jamie Wiebe *et al.*, *Problem Gambling Prevalence Research: A Critical Overview*, report to the Canadian Gaming Association, December 2007, at p. 17,
http://canadiangamingassociation.com/media_uploads/pdf/78.pdf
 (last accessed on July 11, 2009). Also noted in interviews with Matthew Hill, Director of Strategy, Research and Analysis at the British Gambling Commission, Paul Morris, Policy Development Manager at the British Gambling Commission, and Peter Collins, Professor of Public Policy Studies and Director of the Center for the Study of Gambling at the University of Salford (U.K.).

⁸⁰ Noted in an August 5, 2009 interview with Glenn Gibson, Manager of Technical and Systems Audit at the Tasmanian Gaming Commission, and Damien Jarvis, Assistant Director of the Liquor and Gaming Branch of the Tasmania Department of Treasury and Finance (Australia).

⁸¹ See *Supra* at footnote 31 at p. 13 and 21.

all staff in key positions. The regulatory regime could also give aggrieved consumers the ability to bring civil lawsuits and other rights of action against the site.

3. Relevant Technologies for Risk Mitigation

An effective regulatory regime must combine strong and competent oversight with an effective method for lodging complaints with the regulator or law enforcement agencies. In the examples of cheating mentioned above, it was only after private investigations by players that the sites themselves and the regulator responded.⁸² The Kahnawake Gaming Commission, the regulator for both sites noted above, ordered Absolute Poker to institute compliance programs and subject itself to random audits; it also fined the site \$500,000.⁸³ Similarly, the Commission ordered UltimateBet to refund any money owed to players who were victims of cheating, modified UltimateBet's control system, and fined the site \$1.5 million.⁸⁴

Another potential risk-mitigating factor within a regulatory regime is the use of *Mutual Recognition Agreements* (MRAs), which are arrangements between nations to recognize each other's regulatory standards and controls in a particular area of commerce.⁸⁵ Much as the United Kingdom's "White List" permits or denies advertising on the basis of the quality of a jurisdiction's regulatory structure, an MRA could be used as a filter for permitted advertising, for referrals between sites, and even as a way of selectively retaining prohibitions on foreign sites on the basis of quality and integrity rather than the simple fact that they are foreign.

Although both monetary sanctions and regulatory oversight are key to effective regulation, technology offers methods to prevent cheating over and above what is available to land- and river-based casinos. PartyGaming Plc is a publicly-traded Internet gambling company regulated in Gibraltar, and its PartyPoker affiliate holds about an 8% share of the world's market for online poker.⁸⁶ PartyGaming's games and its random number generator are tested by iTech Labs, an independent gaming device tester. It is also a member of the European Gaming & Betting Association and of eCOGRA, both of which publish standards for gaming operators.⁸⁷ 888.com,

⁸² Gilbert M. Gaul, "Players Gamble on Honesty, Security of Internet Betting," *The Washington Post*, November 30, 2008, p. A12.

⁸³ Kahnawake Gaming Commission, *In the Matter of Absolute Poker – Investigation regarding Complaints of Cheating*, January 11, 2008. <http://www.kahnawake.com/gamingcommission/KGC-AP-0111.pdf> (last accessed on July 24, 2009), at p. 4.

⁸⁴ Kahnawake Gaming Commission, Kahnawake Gaming Commission Imposes Sanctions on Ultimate Bet with Regard to Cheating Incidents, September 29, 2008, <http://www.kahnawake.com/gamingcommission/kgc092908.pdf> (last accessed on July 24, 2009).

⁸⁵ See Public Citizen, Mutual Recognition Agreements (MRAs), <http://www.citizen.org/trade/harmonization/MRA/> (last accessed on August 10, 2009).

⁸⁶ As noted in an August 21, 2009 interview with Andrew Fritchie, General Counsel of PartyGaming Plc. Also see <http://www.partygaming.com/prty/en/ourgames/overview/poker> (last accessed on September 10, 2009).

⁸⁷ See http://www.partypoker.com/about_us/ (last accessed on September 10, 2009).

another publicly traded gambling site based in Gibraltar, also uses iTech Labs for verification and is a member of eCOGRA and the Interactive Gaming Council, an online gambling trade group.⁸⁸ Betfair, an Internet betting exchange based in the United Kingdom, is a member of the Independent Betting Adjudication Service, a third-party adjudicator for gambling disputes.⁸⁹

4. Conclusion

As demonstrated above, the most effective system of regulation to combat site operator fraud combines strict enforcement with cooperation by the site operators themselves. Reputable operators with brands to protect could not afford to risk damage to their reputations, loss of their licenses, or regulatory sanctions. However, this incentive is not perfect, and the regulator must be fully equipped to detect and punish site operator fraud. Regulations may be similar to those that apply in the bricks-and-mortar industry. We expect that the online gambling industry will support a supervisory approach that includes regulatory monitoring and sanctions to help promote and maintain an industry reputation for integrity.

C. Cheating or Defrauding of Players by Other Players

As discussed previously, both Absolute Poker and UltimateBet, two popular online poker websites, were rocked by accusations of cheating in 2007 and 2008.⁹⁰ The cheaters were players on the site who had acted in concert with employees of the gambling website. These and other high-profile examples demonstrate the potential for cheating online and the basis for fear among online gamblers of being defrauded by other players. However, a system of regulation promises to rein in such fraudulent activity.

1. The Issue of Players Being Defrauded by Other Players

U.S. gamblers currently lack any effective means to seek remedy from other players for fraud. Because players in the United States engage in online gambling outside of legal and regulatory safeguards, they are unlikely to complain to authorities about cheating experienced on a site: “Individual players are unlikely to volunteer information that would reveal that they have gambled online....Users who doubt the legality of their own actions are unlikely to snitch.”⁹¹

Although the extent of player cheating and fraud is not well documented, it is a common concern for online players.⁹² A 2008 study of Swedish online poker players revealed that one of their

⁸⁸ See <http://www.888.com/> (last accessed on September 10, 2009).

⁸⁹ See <http://content.betfair.com/aboutus/?product=exchange&brand=betfair®ion=GBR&locale=en> (last accessed on September 10, 2009).

⁹⁰ See *Supra* at footnote 5 Bo Bernhard.

⁹¹ See *Supra* at footnote 17 at p. 926.

⁹² John McMullan and Aunshul Rege, *Cheating and Cybercrimes @ Gambling Sites.com*, presentation to the Alberta Gambling Research Institute Annual Conference, March 2009, slide 2.

biggest concerns was being cheated by other players.⁹³ In a 2006 survey, the American Gaming Association reported that 46% of online gamblers believed that other players find ways to cheat.⁹⁴ Finally, the aforementioned 2007 UNLV survey revealed that 63% of respondents were “not at all confident” that other players could not cheat them.⁹⁵ The survey also includes anecdotal evidence from respondents about cheating by players, although evidence on the extent of cheating is generally mixed.⁹⁶

Cheating by players can take various forms:

- *Poker bots* are automated programs that can reportedly play poker at the level of a professional tournament player, using a decision engine utilizing advanced neural network technology.⁹⁷ These bots, such as PokerSmoke, can memorize play styles, recognize betting patterns, and calculate odds, potentially giving those who use them a distinct edge over other players.⁹⁸
- A simpler form of cheating involves *collusion* on online poker tables, in which two or more players work together to share information to gain an unfair advantage over unsuspecting players.⁹⁹
- Another form is *multitabling*, in which a person uses multiple accounts to enter a tournament as two or more different players and garners information in a similar way to collusion; this particular type of cheating is clearly not possible in an offline environment.¹⁰⁰

⁹³ Richard T. A. Wood and Mark D. Griffiths, “Why Swedish People Play Online Poker and Factors that Can Increase or Decrease Trust in Poker Web Sites: A Qualitative Investigation,” *Journal of Gambling Issues*, 21 (July 2008): 80–97 at p. 90.

⁹⁴ See *Supra* at footnote 70.

⁹⁵ See *Supra* at footnote 5 Bo Bernhard at p. 38-39.

⁹⁶ See *Id.* at p. 40–43.

⁹⁷ Mike Bruner, “Poker ‘Bots’ Raking Online Pots?” MSNBC.com, September 21, 2004. <http://www.msnbc.msn.com/id/6002298/print/1/displaymode/1098/> (last accessed on July 25, 2009). Also see *Supra* at footnote 92, slide 7.

⁹⁸ See *Id.*

⁹⁹ Bill Rini, The Definitive Guide to Online Poker Cheating, April 16, 2008. <http://www.billrini.com/2008/04/16/the-definitive-guide-to-online-poker-cheating/> (last accessed on July 25, 2009).

¹⁰⁰ See *Supra* at footnote 68 Christopher Grohman at p. 63.

- The Absolute Poker and UltimateBet cheating cases, mentioned previously, involved players using “superuser” accounts that allowed them to see other players’ hole cards in online poker, making them essentially unbeatable.¹⁰¹
- Hackers can potentially alter sites to ensure winnings or swing odds in their favor, as in a case in 2001 in which hackers rigged games on two gambling sites and managed to win \$1.9 million in just a few hours.¹⁰²

2. Existing Controls in Other Jurisdictions

Although the UltimateBet and Absolute Poker cheating scandals involved participation from insiders at the affected poker sites, it is important to note that both episodes were revealed through the investigative work of other players on the sites.¹⁰³ Although players have an incentive to reveal fraud by other players, some level of regulatory oversight and potential law enforcement involvement is needed to ensure that the site operator takes complaints lodged against players seriously. The regulator could mediate disputes between the site operator and players, independently monitor sites for cheating, and work with site operators to help them prevent cheating. The following are examples of ways that other jurisdictions combat player fraud:

- The British Gambling Commission requires that licensees “put into effect a written procedure for handling customer complaints and disputes” and also have arrangements for disputes to be referred to an independent third party if they are not resolved to the customer’s satisfaction.¹⁰⁴
- Tasmania’s Gaming Commission requires that customer complaints can be made to it and has the power to levy fines and revoke sites’ licenses as well as settle customer disputes. It also has access to the systems of its licensees.¹⁰⁵
- Gibraltar also requires that sites have a formal system to handle customer complaints.¹⁰⁶

¹⁰¹ See *Supra* at footnote 82.

¹⁰² RSe Consulting, *A Literature Review and Survey of Statistical Sources on Remote Gambling*, October 2006, http://www.culture.gov.uk/images/publications/RemoteGambling_RSeReport.pdf (last accessed on July 25, 2009), at p. 20.

¹⁰³ See *Supra* at footnote 65.

¹⁰⁴ See *Supra* at footnote 32 at p. 15.

¹⁰⁵ Noted in an August 5, 2009 interview with Glenn Gibson, Manager of Technical and Systems Audit at the Tasmanian Gaming Commission, and Damien Jarvis, Assistant Director of the Liquor and Gaming Branch of the Tasmania Department of Treasury and Finance (Australia).

¹⁰⁶ See *Supra* at footnote 31 at p. 17–18.

- Sites' own terms of service often explicitly preclude certain potentially fraudulent behaviors.¹⁰⁷

3. Relevant Technologies for Risk Mitigation

As with the issue of fraud by site operators, technology offers solutions to help combat fraud by players. The first line of defense is analysis by other players, who may be in a position to observe aberrant behavior, investigate it, and lodge a complaint with the site operator. However, players may have a hard time detecting cheating as it is occurring, because of the speed and style of online gambling. Site operators, on the other hand, can store large volumes of data on gambling transactions and present them in an easy-to-analyze format, unlike operators of land- and river-based casinos. Analysis of hand histories in poker, for example, may allow operators to identify collusion, the use of poker bots, and other unusual gameplay activities.

The regulator may require that the site operator provide these data at regular intervals for analysis in the event that an inquiry or red flag is triggered. It might also mandate implementation of pattern recognition software to scan routinely for anomalous betting patterns. Finally, the regulator could provide sites' data history to third-party verification companies that conduct their own analyses, including checks for randomness, collusion, and other suspicious patterns.

Clearly, players want to know that their online gambling experience is fair. According to the survey of Swedish poker players, "[t]he response of the operator to [issues of cheating] played a major role in whether or not they were trusted in the long term."¹⁰⁸ Gambling sites, especially reputable ones, have an incentive to control cheating to maintain their good reputation. However, although the revelation of cheating can itself be damaging to a site's reputation, the site can often continue to make money as usual even while players are being defrauded.¹⁰⁹

A regulatory structure, therefore, must balance these contradictory incentives. It must combine strong internal controls by site operators with strict regulatory oversight, perhaps by requiring that mandatory hand history reports or other similar data be submitted to the regulator or through the use of regulator-verified poker bot detection software.¹¹⁰ Also, the regulator could maintain a

¹⁰⁷ For example, multitableting and collusion are considered cheating according to poker room rules. See Christopher Grohman, "Reconsidering Regulation: A Historical View of the Legality of Internet Poker and Discussion of the Internet Gambling Ban of 2006," *Journal of Legal Technology Risk Management*, 1, No. 1 (Fall 2006): 34–74, at p. 63; and Bill Rini, *The Definitive Guide to Online Poker Cheating*, April 16, 2008, <http://www.billrini.com/2008/04/16/the-definitive-guide-to-online-poker-cheating/> (last accessed on July 25, 2009).

¹⁰⁸ See *Supra* at footnote 93 at p. 90.

¹⁰⁹ As in the UltimateBet and Absolute Poker scandals. Also see *Supra* at footnote 97 Mike Bruner.

¹¹⁰ For example, bwin has dedicated staff that deploy "[s]tate-of-the art systems [that] are used to analyze hands and to detect chip dumping, collusion or the use of poker bots." From an August 13, 2009 correspondence with Katharina Riedl of bwin (Austria).

database of known cheaters, and sites' own verification processes could help exclude such gamblers at the point of registration. This strategy also has the benefit of preventing cheaters from skipping easily from one website to another. Regulation could also grant players the right to bring a civil claim against a gambling site for not preventing cheating by its users, providing additional incentives for sites to implement effective controls.¹¹¹

4. Conclusion

Site operators, players, and regulators share an interest in detecting and protecting against player fraud. This naturally leads to cooperative regulatory oversight. Such oversight would recognize the inherent opportunities in the online environment for comprehensive data storage, allowing a level of analysis to detect fraud that is unavailable in the bricks-and-mortar environment. Consequently, legal, regulated online gambling should provide greater protections against player fraud than does the current environment.

D. Involvement of Organized Crime in Gambling Operations

Casino gambling, in which nearly all transactions are in cash, is particularly susceptible to *skimming*, in which profits are removed by the owners or other insiders before being declared, as well as money laundering.¹¹² Moreover, its illegal status in many jurisdictions implies that those who offer gambling services in those jurisdictions are, by definition, law breakers. Online gambling, however, presents different challenges and opportunities than does its bricks-and-mortar counterpart. On the one hand, identities can be easier to conceal online, transactions can occur far from where regulators are located, and members of collaborating crime networks can be located in far-flung locations.¹¹³ On the other hand, online transactions are easier to aggregate and analyze, providing richer opportunities to detect the operations of organized crime groups.¹¹⁴ The lack of cash transactions makes auditing and the detection of skimming easier than in a bricks-and-mortar environment.

1. The Issue of Involvement of Organized Crime in Online Gambling

Organized crime has been largely eliminated from bricks-and-mortar casinos.¹¹⁵ In Nevada, for example, the regulatory regime has largely eliminated criminals from the ownership of

¹¹¹ See *Supra* at footnote 68 at p. 67–68.

¹¹² Jay Albanese, “Casino Gambling and Organized Crime: More Than Reshuffling the Deck,” in *Contemporary Issues in Organized Crime*, edited by Jay Albanese (Monsey, New York: Criminal Justice Press, 1995). Also see Kevin B. Kinnee, *Practical Gambling Investigation Techniques* (New York: Elsevier, 1992), at p. 3–5.

¹¹³ See *Supra* at footnote 63 at p. 128.

¹¹⁴ As noted in an August 5, 2009 interview with Phill Brear, Head of Gambling Regulation at the Gibraltar Regulatory Authority, online gambling allows a perfect audit trail to be kept.

¹¹⁵ Jay Albanese, “Casino Gambling and Organized Crime: More Than Reshuffling the Deck,” in *Contemporary Issues in Organized Crime*, edited by Jay Albanese (Monsey, New York: Criminal Justice Press, 1995), at p. 4–5.

casinos.¹¹⁶ Another factor in the Nevada transformation has been the introduction of large, publicly held companies as casino owners, which cannot afford associations with organized crime.¹¹⁷ The same effect may hold true for online gambling enterprises, some of which are already publicly traded.

In the past, when organized crime had been involved in bricks-and-mortar casinos, it traditionally controlled the gambling organization itself, usually behind the presence of a front man in cases of legal gambling establishments.¹¹⁸ Similarly, gambling websites could be controlled by organized syndicates. Finally, as discussed more fully in Section F, criminals can use online gambling for the purpose of money laundering.

2. Existing Controls in Other Jurisdictions

In bricks-and-mortar casinos, background checks and verification for site operators and employees are standard procedures across all jurisdictions in the United States. In New Jersey, those who wish to operate a casino are required to obtain a casino license.¹¹⁹ Applicants must prove their financial stability and integrity; the financial integrity of their investors or backers; their good character, honesty, and integrity; and their business ability and casino experience. They must also submit to a criminal background check.¹²⁰ Each casino employee must obtain a valid casino employee license, which involves providing his or her name, address, and fingerprints; and to consent to a criminal background check, which the New Jersey State Police performs at the applicant's expense.¹²¹ The State Police are also obliged to notify the New Jersey Division of Gaming Enforcement if a license holder is arrested at any point after the initial background check.¹²² To eliminate small gambling establishments, casinos in Atlantic City are required to have a minimum of 500 hotel rooms, and all games are tightly regulated and controlled. Also, those that provide a certain amount of ancillary services (such as cleaning, food, construction, and security) to casinos must be licensed and submit to background checks.¹²³

Similarly, Nevada laws impose on operators of gambling establishments licensing requirements that require that the applicant (1) be a person of good character, honesty, and integrity; (2) be a person whose prior reputation and criminal record do not pose a threat to the public interest of

¹¹⁶ See *Id.* at p. 4.

¹¹⁷ See *Id.* at p. 7–8.

¹¹⁸ See *Id.* at p. 3.

¹¹⁹ New Jersey Permanent Statutes, Title 5, Amusements, Public Exhibitions and Meetings, 5:12-82: Casino license – applicant eligibility.

¹²⁰ *Id.* at 5:12-84: Casino license – applicant requirements.

¹²¹ See *Id.*

¹²² See *Id.*

¹²³ See *Supra* at footnote 115 at p. 10.

the state or of its gambling regulations; and (3) have sufficient financial resources and business acumen to operate the establishment.¹²⁴ Employees in general are required to register as gaming employees, to submit fingerprints, and to be subjected to an FBI background check. The Nevada Gaming Control Board is empowered to object to any applicant for “any cause deemed reasonable.”¹²⁵

Many jurisdictions across the world that license online gambling include provisions for checks on the site’s operators. The following are examples of such provisions:

- In the Isle of Man, the Gambling Control Commission has the duty “[t]o investigate the character and financial status of persons behind online gambling operations.”¹²⁶
- The U.K. Gambling Act of 2005 allows the Gambling Commission, when issuing a license, to consider “the integrity of the applicant or of a person relevant to the application” and to refuse a license to a person convicted of a “relevant offence.”¹²⁷
- Alderney’s Gambling Control Commission has the duty to “determine whether an applicant is ‘fit and proper’ to hold a license. Investigations can include interviews with key individuals, and the Commissioners may also require their own meeting with representatives of the applicant before deciding whether to grant a license.”¹²⁸ The regulator also requires that business associates of site operators and software providers hold licenses.¹²⁹
- Tasmania’s Gaming Commission conducts thorough probity investigations on site operators, including credit checks and fingerprint background checks; the checks are also required for employees of the gambling website.¹³⁰

¹²⁴ Nevada Revised Statutes, Chapter 463.170.

¹²⁵ *Id.* at Chapter 463.335.

¹²⁶ See *Supra* at footnote 30 at p. 128.

¹²⁷ Gambling Act, 2005 Chapter 19 (Eng.), at §§70–71, http://www.opsi.gov.uk/acts/acts2005/pdf/ukpga_20050019_en.pdf (last accessed on September 11, 2009).

¹²⁸ See *Supra* at footnote 29 at p. 140–141.

¹²⁹ Noted in an August 27, 2009 interview with André Wilsenach, Chief Executive Officer of the Alderney Gambling Control Commission.

¹³⁰ As noted in an August 5, 2009 interview with Glenn Gibson, Manager of Technical and Systems Audit at the Tasmanian Gaming Commission, and Damien Jarvis, Assistant Director of the Liquor and Gaming Branch of the Tasmania Department of Treasury and Finance (Australia).

- The regulator in Australia’s Northern Territory checks the reputation of operators and their associates and proposed managers, as well as operators’ financial background, resources, and business ability.¹³¹
- Gibraltar’s Gambling Act 2005 prevents the licensing authority from granting a license to a person who is not “fit and proper” or if granting the license would be against the public interest. The Gambling Act allows the regulator to take into account the licensee’s character, honesty, and integrity, as well as his or her reputation, business plan, experience, and other factors.¹³²

As can be seen, each jurisdiction considers the exclusion of criminals to be essential to maintaining an effective regulatory regime.

3. Relevant Technologies for Risk Mitigation

Any regulatory regime that wishes to exclude criminals must focus on erecting sufficiently high barriers to entry.¹³³ Simple techniques such as requiring background checks, interviews, and letters of reference can familiarize the regulator with its license applicants and allow it to make a more informed decision on whether to grant a license. This level of investigation of site operators could extend to owners, beneficiaries, business associates, managers, and security personnel.¹³⁴ Rigorous vetting of new applicants can combine with ongoing compliance checks to ensure that once a license is granted, it is not clandestinely transferred to criminal control.

4. Conclusion

Although criminal control of gambling websites is a possibility, strict regulation would exclude unwanted site operators. It is unlikely that criminals would subject themselves to strict regulatory checks and demanding admission standards. Instead, they may attempt to operate gambling sites without licenses. Regulators can work to educate consumers about the dangers associated with unlicensed websites, and steer them toward licensed, regulated sites which offer protection against criminal activity. At the risk of losing their licenses, legitimate operators would have a strong interest in avoiding ineligible associates as is the case with bricks-and-mortar casinos. We would expect legitimate, licensed sites to be receptive to a fair degree of scrutiny because such scrutiny would enhance the reputation of the industry.

¹³¹ As noted in an August 31, 2009, correspondence with John Sealy, Manager of Information Systems and Technology Services at the Licensing, Regulation and Alcohol Strategy division of the Northern Territory Department of Justice (Australia).

¹³² Gibraltar Gambling Act 2005, Schedule 1, at §3, <http://www.gra.gi/sites/gambling/downloads/42/gambling%20ord%202005.pdf> (last accessed on August 6, 2009).

¹³³ See *Supra* at footnote 29 at p. 140.

¹³⁴ See *Id.*

E. Money Laundering by Players

A major concern of law-enforcement authorities is money laundering facilitated by online gambling.¹³⁵ However, many financial analysts believe that the risks of money laundering in online gambling is low because electronic transactions are closely monitored and recorded.¹³⁶ A combination of anti-money-laundering regulations, currently in place for bricks-and-mortar casinos as well as other financial institutions, and the use of technology would provide the online gambling environment with better opportunities for detecting money laundering by players than those available in land- and river-based casinos.

1. The Issue of Money Laundering by Players

Money laundering is a process through which proceeds derived from illegal activity are legitimized.¹³⁷ Money laundering is typically accomplished in three stages: (1) the placement stage, (2) the layering stage, and (3) the integration stage.¹³⁸ The *placement* stage is defined as the first entry of illegal money into financial institutions or the retail economy. The *layering* stage consists of activities meant to hide the trail of money, generally involving the transfer of money among multiple entities. The final stage, the *integration* stage, is when the illegal funds are reintroduced into the economy to appear as though they were legitimate. It is difficult for law enforcement to detect this reintroduction of illicit funds into the economy without an audit trail established during the first two stages of the laundering process.¹³⁹

The following (hypothetical) example demonstrates how online gambling websites can be used to launder money: A customer could establish an Internet gambling account under a false name and use illicit funds to conduct a minimal amount of betting. After a few losses, the customer could request repayment from the Internet gambling site and claim them as winnings, thereby creating a legitimate source for the remaining funds.¹⁴⁰

The U.S. Department of Justice is concerned that online gambling offers criminals an easy vehicle for money laundering because of its anonymous nature, use of encryption, volume,

¹³⁵ Government Accountability Office, *Internet Gambling: An Overview of the Issues*, GAO-03-89, December 2002, at p. 34–37.

¹³⁶ See *Id.*, at p. 37–38.

¹³⁷ Mark D. Schopper, “Internet Gambling, Electronic Cash & Money Laundering: The Unintended Consequences of a Monetary Control Scheme,” *Chapman Law Review*, 5, No. 1 (2002): 303-330.

¹³⁸ Financial Crimes Enforcement Network, *The SAR Activity Review – Trends, Tips & Issues*, May 13, 2008, http://www.fincen.gov/news_room/rp/files/sar_tti_13.pdf (last accessed on August 5, 2009).

¹³⁹ See *Supra* at footnote 137.

¹⁴⁰ Testimony of John G. Malcolm Before the Committee on Banking, Housing, and Urban Affairs, March 18, 2003, <http://www.usdoj.gov/criminal/cybercrime/malcolmTestimony318.htm> (last accessed on September 11, 2009). Also see *Supra* at footnote 135.

speed, international reach, and offshore locations.¹⁴¹ In his testimony before Congress in 2003, Deputy Assistant Attorney General John G. Malcolm noted that e-casinos are an excellent vehicle for money laundering because in addition to using the gambling services offered to hide or transfer money, online gambling websites offer a wide variety of financial services to their customers, including credit accounts, fund transmittal services, check cashing services, and currency exchange services.¹⁴²

There is little documentation by which to gauge the extent of actual money laundering in online gambling. In 2002, the U.S. General Accounting Office (GAO) examined the vulnerability of online gambling to money laundering and concluded that the “views on the vulnerability of Internet gambling to money laundering are mixed.”¹⁴³ Its report provides only hypothetical examples of how online gambling sites could be used to launder money and does not describe any actual cases. A 2005 report prepared for the Interactive Gaming Council in Canada calls evidence of the existence of money laundering in online gambling “scant” and claims that the Internet Crime Complaint Center had never logged a complaint of money laundering through gambling sites.¹⁴⁴ It goes on to claim that “Internet gaming does not, in and of itself, contribute to money laundering. Rather, it is the financial transactions that are used to move money on the Internet that may be susceptible to money laundering.”¹⁴⁵

One can understand money laundering patterns that might occur in online gambling by extrapolating from the patterns of money laundering seen in bricks-and-mortar casinos. Various betting patterns associated with money laundering in bricks-and-mortar casinos have been identified, including the use of hedged bets by colluding players, light betting or *minimal play* (i.e., using bets that are small relative to the size of deposits and withdrawals), splitting transactions up into units smaller than reporting thresholds, splitting transactions across reporting “days,” and pressuring staff to not comply with their reporting obligations.¹⁴⁶

A problem related to money laundering is that of terrorist financing, in which funds that are intended for terrorist groups are moved through the financial system in an apparently legitimate way. Effective anti-money-laundering provisions must specifically address the risks of terrorist financing, although many techniques to combat money laundering are also effective against

¹⁴¹ See *Id.* John G. Malcolm.

¹⁴² See *Id.*

¹⁴³ See *Id.*

¹⁴⁴ NFC Global, “Internet Gaming & Money Laundering: Measuring the Scope, Assessing the Risks,” Prepared for the Interactive Gaming Council, Vancouver, British Columbia, Canada, August 2005, at p. 4.

¹⁴⁵ See *Id.*

¹⁴⁶ American Gaming Association, Suspicious Activity Reporting Policy, [http://www.americangaming.org/assets/files/SARC_Policy_\(6\).pdf](http://www.americangaming.org/assets/files/SARC_Policy_(6).pdf) (last accessed on July 28, 2009).

terrorist financing.¹⁴⁷ The only known case of money laundering through gambling sites was related to terrorist financing: in 2007, a suspected terrorist named Al-Daour used stolen credit cards to deposit funds at 43 different gambling sites and then withdrew the winnings to various online bank accounts.¹⁴⁸

2. Existing Controls in Other Jurisdictions

Congress has enacted legislation to detect money laundering. Under the Bank Secrecy Act (BSA) of 1970, all U.S. financial institutions, including banks, credit unions, securities firms, and casinos, are required to report large currency transactions and suspicious activities.¹⁴⁹ The Financial Crimes Enforcement Network (FinCEN) administers these regulations. The casino gambling industry has been covered by the BSA since 1985, and FinCEN has specific regulations that pertain to casino gaming. The BSA requires the reporting of any currency transactions exceeding \$10,000 in a single gaming day on a Currency Transaction Report (CTR).¹⁵⁰ Because money launderers can structure transactions such that they never result in a CTR being filed, all land- and river-based casinos are also required to file Suspicious Activity Reports (SARs). Casinos have to file SARs if they know, suspect, or have reason to suspect that a transaction involving \$5,000 or more meets certain criteria, including involvement of illicit funds, intention to avoid or prevent proper reporting, exhibiting of abnormal behavior, or use of the casino to facilitate criminal activity.¹⁵¹

The leading online gambling jurisdictions have created regulatory structures that resemble traditional regulation for land- and river-based casinos in the United States. These jurisdictions require some form of anti-money-laundering monitoring, ranging from restricting customers to a single account to identifying and reporting suspicious transactions or players' abnormal betting patterns.¹⁵²

In addition to regulation that combats money laundering in its financial services sector, the Isle of Man has put in place the Anti-Money Laundering Code to prevent money laundering through gambling websites.¹⁵³ Operators are required to comply with strict anti-money-laundering

¹⁴⁷ MHA Consulting, *The Threat of Money Laundering and Terrorist Financing through the Online Gambling Industry*, report prepared for the Remote Gambling Association, June 2009, at p. 6–8.

¹⁴⁸ See *Id.* at p. 31.

¹⁴⁹ American Gaming Association, *Money Laundering*, AGA Fact Sheet, http://www.americangaming.org/Industry/factsheets/issues_detail.cfv?id=3 (last accessed on September 11, 2009).

¹⁵⁰ See *Id.*

¹⁵¹ See *Id.*

¹⁵² David O. Stewart, *An Analysis of Internet Gambling and Its Policy Implications*, AGA 10th Anniversary White Paper Series on Internet Gambling, 2006.

¹⁵³ See *Supra* at footnote 30 at p. 126–127.

procedures, which include identification of prospective customers, evidence of identity, changes to patterns of transactions, record keeping, records of transactions, retention of records, reporting suspicious transactions, and training.¹⁵⁴ In addition, site operators are legally required to report any suspicious transactions to the Financial Crime Unit (FCU). Specialized software can flag these transactions.

Similarly, to combat money laundering, Alderney requires operators of online gambling websites to implement business risk assessments, customer due diligence procedures, monitoring of transactions and other activity, suspicious activity reporting procedures, employee screening and training procedures, and record-keeping procedures.¹⁵⁵

3. Relevant Technologies for Risk Mitigation

An anti-money-laundering regulatory regime for online gambling may be modeled on the current regulatory structure for traditional bricks-and-mortar casinos. A regulatory framework for online gambling may leverage the technological environment for online gambling and require (1) preservation of an audit trail of transactions for analysis by federal authorities; (2) implementation of customer identification standards; (3) controls to prevent anonymous, structured transactions; (4) establishment of an anti-money-laundering compliance program; (5) training for all appropriate personnel; and (6) compliance with all relevant BSA requirements.¹⁵⁶

The IGC notes that “online gambling, with a combination of regulatory oversight and use of technology—while facing the same threats as real-world gambling facilities—is in a better position to address these risks.”¹⁵⁷ For example, all electronic fund transfers can be electronically recorded, thus providing a detailed and automatic transaction trail not currently available in land- and river-based casinos.¹⁵⁸

The IGC further notes that a basic requirement to combat money laundering is to “know your customer.” Stringent player registrations and ongoing verification processes combined with appropriate regulatory oversight and banking regulations help fulfill this requirement.¹⁵⁹ Italy’s regulatory regime, for example, requires a potential customer to submit a signed contract along with a copy of his or her identification.¹⁶⁰ Tasmania requires strong identity verification

¹⁵⁴ See *Id.*

¹⁵⁵ See Alderney Gambling Control Commission, *The Alderney eGambling Regulations*, 2006., <http://www.gamblingcontrol.org/userfiles/file/97.pdf> (last accessed on August 19, 2009), at Schedule 6, Part VI.

¹⁵⁶ See *Id.*

¹⁵⁷ Interactive Gaming Council, “Online Gambling Sites Less Susceptible to Money Laundering Than Real-World Counterparts,” *Winner Online*, September 24, 2002, <http://www.winneronline.com/articles/september2002/fatf.htm> (last accessed on September 11, 2009).

¹⁵⁸ See *Supra* at footnote 114.

¹⁵⁹ See *Supra* at footnote 114.

¹⁶⁰ As noted in an August 13, 2009 correspondence with Katharina Riedl of bwin (Austria).

procedures to be in place on player accounts.¹⁶¹ Moreover, technology can equip site operators with tools to scrutinize inconsistent player behavior, and then capture and report the transaction.¹⁶²

Another essential anti-money-laundering measure noted by the IGC is to require that gamblers be paid any winnings in the same way in which the money was originally deposited.¹⁶³ This system allows an audit to track transfers of funds much more easily and removes the ability of launderers to use an account as a pass-through for funds.¹⁶⁴ Also, care must be taken when allowing transfers of funds between players, which could potentially be a conduit for money laundering. Alderney's money laundering guidance suggests that transferred funds be allowed only for gambling and not for withdrawal or that site operators undertake further due diligence on players involved in transfers.¹⁶⁵

In addition to a system modeled on requirements for bricks-and-mortar gambling, a regulator can require the same procedures that are required of online merchants, banks, and payment providers. In Europe, online gambling operators have been bound by these requirements since 2003 under the Third European Money Laundering Directive.¹⁶⁶ U.S. licensed operators would also be bound by relevant anti-money-laundering requirements. Most nations are also subject to the recommendations of the Financial Action Task Force, an international body formed to combat money laundering and terrorist financing. Each nation may also have its own money laundering regulations, such as the United Kingdom's Money Laundering Regulations, which cover both financial and nonfinancial businesses.¹⁶⁷

Although financial businesses are still subject to the most stringent regulation, all of these regulations use a risk-based approach, in which the level of scrutiny of transactions is commensurate with the risk of money laundering in those transactions.¹⁶⁸ The most important aspects of financial companies' risk mitigation involve three broad activities: (1) "know your customer" procedures, (2) monitoring for suspicious activity, and (3) procedures for reporting suspicious activity.¹⁶⁹ Identity verification can involve both paper and electronic identification,

¹⁶¹ As noted in an August 5, 2009 interview with Glenn Gibson, Manager of Technical and Systems Audit at the Tasmanian Gaming Commission, and Damien Jarvis, Assistant Director of the Liquor and Gaming Branch of the Tasmania Department of Treasury and Finance (Australia).

¹⁶² See *Id.*

¹⁶³ See *Supra* at footnote 157.

¹⁶⁴ See *Supra* at footnote 147 at p. 26.

¹⁶⁵ *Id.* at p. 20.

¹⁶⁶ *Id.* at p. 1.

¹⁶⁷ *Id.*

¹⁶⁸ *Id.* at p. 2.

¹⁶⁹ *Id.* at p. 29–31.

and the level of additional identification required rises with the risk in the particular industry and transaction. Suspicious activity monitoring involves standard procedures that are designed to reveal signs of monitoring while retaining privacy protection. All suspicious activity must be reported to law enforcement, which takes over the investigation immediately. Suspicious activity reporting, as part of the regulations, is the responsibility of all company staff members, who must be trained in the signs of money laundering and be able to report their suspicions expeditiously. In the United Kingdom, not reporting suspected money laundering is a criminal offense with a maximum sentence of two years in prison.¹⁷⁰

4. Conclusion

Players or groups of players acting in concert may attempt to use legitimate gambling operations for money laundering. To curb such activities, regulators could subject online gambling operators to anti-money-laundering regulations that are currently in place for bricks-and-mortar casinos and for online merchants, banks, and payment providers. The online environment provides better opportunities for detecting money laundering by players or player groups than do bricks-and-mortar casinos.

In an effective anti-money-laundering regime, site operators would be required to retain comprehensive data on all deposits, withdrawals, and betting transactions and to make these available to regulators for examination and analysis. Given complete data, most patterns related to money laundering (such as light betting or matched bets placed by collaborators) would be easier to detect than they are in a physical environment (where complete transaction histories are available only in the form of video recordings).¹⁷¹ Software for detecting anomalies and suspicious behavior may be operated easily and routinely on digital databases by operators, regulators, or both.

The site operators' obligations with respect to their own detection of money laundering would form a part of their ordinary compliance obligations under such a licensing regime. Because of the absence of cash in online gambling transactions, the auditable record that is created, and the regulator-imposed reporting requirements for most transactions, it is likely that site operators can prevent money laundering by players and terrorist financing at least as effectively as can bricks-and-mortar casinos.¹⁷² In contrast, the current prohibitions related to online gambling forces players to use unconventional forms of payment that leave harder-to-follow audit trails, and may therefore increase the risk of money laundering.

¹⁷⁰ *Id.* at p. 23.

¹⁷¹ As noted in an August 5, 2009 interview with Phill Brear, Head of Gambling Regulation at the Gibraltar Regulatory Authority.

¹⁷² As noted in an August 3, 2009 interview with Paul Mathews, Former Senior Vice President of IGT Wagerworks.

F. Money Laundering by Site Operators

In addition to money laundering by players, there are concerns about money laundering by site operators.¹⁷³ The volume, speed, and international reach of Internet transactions, along with the offshore location of many Internet gambling sites, increase the potential for misuse of these sites by operators for laundering money. As such behavior would constitute criminal conduct by site operators, effective management of the problem involves regulatory restrictions designed to keep criminals out of the Internet gambling industry.

1. The Issue of Money Laundering by Site Operators

The GAO reported in 2002 that U.S. law-enforcement officials believed money launderers might develop Internet gambling sites for the sole purpose of laundering money.¹⁷⁴ GAO sited the possibility that a gambling site operator could design software to skim a percentage of customer deposits and cloak the transactions as gaming losses. In reality these deductions would serve as the operator's service fee for laundering illicit funds. An alternate scenario might involve a gambler transferring funds to the site operator or to a collaborator within the e-casino by continuing to play until he loses the requisite amount. Conversely, if the site operator wanted to transfer funds to a gambler, the games could be rigged so the gambler won.¹⁷⁵

Two recent cases, involving NETeller and playwithal.com, highlight the possibility of online gambling operators using third-party conduits to engage in money laundering, concealing the true nature and purpose of financial transactions. In early 2007, the founders of NETeller, a popular third party payment processor based in the Isle of Man, were arrested and charged with laundering billions of dollars of Internet gambling proceeds.¹⁷⁶ In 2006, the Federal Bureau of Investigation (FBI) began investigating how NETeller processed payments and helped facilitate sports bets. NETeller used payment and shell companies to process Automatic Clearinghouse (ACH) transactions, thus hiding the nature of payments made to U.S. customers. To get money out of the United States, NETeller would have a payment service company receive funds on its behalf and transfer the funds to an account controlled by NETeller in Alberta, Canada.

In the case involving playwithal.com, a sports betting website, 27 people were charged with numerous counts, including money laundering.¹⁷⁷ The defendants were accused of laundering

¹⁷³ General Accounting Office, *Internet Gambling: An Overview of the Issues*, GAO-03-89, December 2002, at p. 36.

¹⁷⁴ See *Id* at p. 37.

¹⁷⁵ Testimony of John G. Malcolm Before the Committee on Banking, Housing, and Urban Affairs, March 18, 2003, <http://www.usdoj.gov/criminal/cybercrime/malcolmTestimony318.htm> (last accessed on July 29, 2009).

¹⁷⁶ Verrinder, Matthew, *NETeller Ex-directors on Money Laundering*, January 16, 2007, <http://www.reuters.com/article/internetNews/idUSN1622302920070116> (last accessed on September 11, 2009).

¹⁷⁷ Online Gambling Operations in Queens Busted, November 16, 2006, <http://online.casinocity.com/article/online-gambling-operation-in-queens-busted-68919> (last accessed on September 11, 2009).

and stashing away millions of dollars using shell corporations and bank accounts in Central America, the Caribbean, Switzerland, and Hong Kong.

2. Existing Controls in Other Jurisdictions

The United States has already enacted strict regulations to detect and deter money laundering, and site operators should clearly be forced to comply. Control strategies for this risk thus focus on keeping organized crime, other criminals and criminal behavior out of the industry.¹⁷⁸ As for all the other concerns about criminal conduct by operators, regulators will set a high bar for initial qualification and conduct periodic reviews of key personnel and their associations. Other jurisdictions do this already. The Isle of Man, U.K., and Alderney assess the suitability of license applicants and require them to submit documentation to satisfy the enforcement authorities that they are persons of good character, honesty and integrity.¹⁷⁹ Operators in these jurisdictions are also required to provide comprehensive financial statements and internal accounting records for audit.¹⁸⁰

In many U.S. states, background checks and employee verification are already standard procedure for bricks-and-mortar casinos. For example, in New Jersey and Nevada, to obtain a license, each casino employee must supply his or her name, address, fingerprints, and consent to a criminal background check.¹⁸¹ Bricks-and-mortar casinos are also required to provide periodic financial reports at a level of detail and in formats specified by regulators.¹⁸²

3. Relevant Technologies for Risk Mitigation

Effective strategies to combat money laundering by site operators involve frequent and comprehensive auditing, the application of pattern recognition to aggregated financial transaction data, and exclusion of criminals.

¹⁷⁸ McCormick, Amanda, *Review of Online Gambling Literature*, British Columbia Center for Social Responsibility, 2007.

¹⁷⁹ Testimony of Mary Williams, in U.S. House of Representatives, Committee on Financial Services, *Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?* 110th Cong., 1st Session, June 8, 2007, p. 128. Also see *Supra* at footnote 127. Also see Testimony of André Wilsenach, in U.S. House of Representatives, Committee on Financial Services, *Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?* 110th Cong., 1st Session, June 8, 2007, at p. 140–141.

¹⁸⁰ Testimony of Mary Williams, in U.S. House of Representatives, Committee on Financial Services, *Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?* 110th Cong., 1st Session, June 8, 2007, at p. 126–127.

¹⁸¹ New Jersey Permanent Statutes, Title 5, Amusements, Public Exhibitions and Meetings, 5:12-82: Casino license – applicant eligibility. Also see Nevada Revised Statutes, Chapter 463.335.

¹⁸² See *Id* Nevada Revised Statutes at Chapter 463.156–159.

4. Conclusion

As with the prevention of fraud and any other criminal conduct by site operators, an effective regulatory regime would seek to bar criminals from entering the Internet gambling industry, and seek to detect and prevent linkages developing between site operators and criminal organizations. Regulators would also develop the capacity to search for laundering patterns among the betting transaction data, as well as among the external financial flows data for regulated sites. Regulators of the online gambling industry would also become natural partners for the broader law-enforcement community seeking to detect and prevent money laundering.

G. Violation of Jurisdictional Restrictions or Prohibitions

A key concern of some policymakers is the ability of regulated online gambling sites to adhere to various jurisdictional restrictions and prohibitions.¹⁸³ For example, with bricks-and-mortar casinos, some states have complete prohibitions (e.g., Utah) while others have legalized most forms of gambling (e.g., Nevada).¹⁸⁴ Add to this mix the numerous Native American tribal areas, and a complicated multilayered jurisdictional map emerges. This section does not comment on federalism or the appropriateness of various levels of jurisdictional control over online gambling. Rather, we look at the ability to ensure through federal regulation that restrictions and prohibitions imposed at various other jurisdictional levels continue to be respected.

1. The Issue of Violation of Jurisdictional Restrictions

A central issue in the debate over legalization of online gambling pertains to different jurisdictions' abilities to preclude gambling website operators from operating from, or serving customers within, specific states or territories.¹⁸⁵

Federal laws, such as the Wire Act and the UIGEA, removed some aspects of states' ability to choose legalization and regulation.¹⁸⁶ On the one hand, the passage of the UIGEA in 2006

¹⁸³ In October 2008, Governor Steve Beshear of Kentucky initiated a lawsuit against gambling sites serving customers in Kentucky; a court ordered 141 website domain names to be transferred to the state's control. The case was later overturned on appeal in January 2009 and is currently being appealed to the Kentucky Supreme Court. In April 2009, the state of Minnesota sent notice to 11 Internet service providers (ISPs) seeking to force them to block access to gambling sites for Minnesota residents. In June, the state rescinded its order. See *Poker News Daily*, "Minnesota Rescinds Internet Gambling Notices to ISPs after iMEGA Settlement," June 8, 2009, <http://www.pokernewsdaily.com/minnesota-rescinds-internet-gambling-notices-to-isps-after-imega-settlement-2749/> (last accessed on August 10, 2009).

¹⁸⁴ American Gaming Association, *States with Gaming*, AGA Fact Sheet, http://www.americangaming.org/Industry/factsheets/general_info_detail.cfv?id=15 (last accessed on July 21, 2009).

¹⁸⁵ Kevin F. King, "Cutting Internet Gambling's Gordian Knot: Geolocation and Federalism on the Internet," *Northwestern University Law Review*, July 14, 2009, <http://ssrn.com/abstract=1433634> (last accessed on July 20, 2009).

increased the federal government's control over online gambling and restricts users' ability to fund their online accounts, casting a broad net over any state attempts to legalize online gambling.¹⁸⁷ On the other hand, states have no recourse against offshore sites that provide gambling services to their residents.¹⁸⁸

Despite concerns that the legalization of online gambling would override various jurisdictions' rights to regulate gambling, technology can give states that opt out of legalization some assurance that their restrictions will be enforced.¹⁸⁹ A well-crafted federal regulatory regime could respect jurisdictional differences with regard to legalization of online gambling.

2. Regulatory Strategy

Proposed legislation provides for the ability of states and Native American tribal groups to opt out of legalization.¹⁹⁰ A federal licensing system would need to ensure (1) that site operators "adopt and implement systems to enforce any applicable Federal, State, and Indian tribe limitations on Internet gambling" and (2) that license applicants have a program "to verify the State or tribal land in which the customer is located at the time the customer attempts to initiate a bet or wager."¹⁹¹ Further, currently proposed legislation prohibits licensees only from "knowingly" accepting bets from jurisdictions that opt out, presumably to prevent state actions against operators for mere negligence.¹⁹² It would be possible to press operators further, requiring them to acquire and operate state-of-the-art methods in this area, effectively guaranteeing their "knowledge" in all but the most unusual of circumstances.

A regulatory strategy to solve jurisdictional issues must entail oversight by a regulator that can monitor site operators, including the use of mystery shopper, to ensure compliance. Beyond that, however, the issue of different jurisdictional restrictions or prohibitions is essentially a technical question: does the technology exist to implement such restrictions or prohibitions?

¹⁸⁶ See *Id.* at p. 2–5.

¹⁸⁷ See *Supra* at footnote 17 at p. 933.

¹⁸⁸ See *Id.* at p. 930.

¹⁸⁹ Spencer Bachus, "Online Gambling Leads to Crime and Hurts Young, So Why Encourage It? Asks Spencer Bachus," *US News & World Report*, June 1, 2009, <http://www.usnews.com/articles/opinion/2009/06/01/online-gambling-leads-to-crime-and-hurts-young-so-why-encourage-it-asks-spencer-bachus.html> (last accessed on July 30, 2009).

¹⁹⁰ "There is a need to extend the regulatory provisions of this Act to all persons, locations, equipment, practices, and associations related to Internet gambling, with each State and Indian tribe having the ability to limit Internet gambling operators from offering Internet gambling to persons located within its territory by opting out of the provisions of this Act" (Internet Gambling Regulation, Consumer Protection, and Enforcement Act, H.R. 2267, 111th Cong. (2009), §5381, ¶6).

¹⁹¹ See *Id.* at §5381, ¶5. Also see *Id.* at §5384(b)(1).

¹⁹² See *Id.* at §5386(a)(1)(A). Also see *Supra* at footnote 185 at p. 17.

3. Relevant Technologies for Risk Mitigation

Many technologies are available to mitigate the risks of jurisdictional violations of restrictions or prohibitions.

To adhere to UIGEA restrictions that prohibit funding of online gambling accounts, some overseas gambling operators, such as PartyGaming, Sportingbet, and Paradise Poker, have used geolocation techniques to selectively deny services to their customers on the basis of their location within the United States.¹⁹³ Similar technology may also be applied to help address the problem of jurisdictional differences in gambling law within the United States.

Geolocation entails using “Internet infrastructure information to determine the geographic location of Internet Protocol (IP) addresses associated with Internet-connected devices.”¹⁹⁴ It is a way of determining the physical location of an Internet user, with varying degrees of accuracy. When an Internet user types a website address into a Web browser, the browser sends an access request to the server of the requested website. This request reveals the IP address of the user, which the requested website forwards to a geolocation provider. The provider, which has built a database of the locations of IP addresses, assesses the location of the user. Public-source geolocation data can often identify the location of IP addresses at the country, state, and even city levels.¹⁹⁵

Gambling websites would, of course, require initial registration information from their users, including the users’ name and address. This is the first line of defense against jurisdictional concerns, because a person attempting to register with a Utah address, for example, would be precluded from opening an account.¹⁹⁶ This information can be cross-checked against supplied information, such as credit card information, bank account numbers, driver’s license details, or passport information to determine any mismatch in the reported location.¹⁹⁷ Players from excluded jurisdictions, or ones whose physical location cannot be verified, can summarily be prevented from opening an account.

This process should serve as a deterrent to casual users in prohibited jurisdictions who do not intend to circumvent the laws of their jurisdiction. Subsequently, however, the site must use geolocation to ensure that users, even if they were eligible at registration, are in a permitted

¹⁹³ See *Supra* at footnote 59, at ¶¶34–36.

¹⁹⁴ Quova, *The Factors of Geolocation*, iGaming Business, <http://gw.vtrenz.net/index.cfm?method=cMicrositeSecurity.displayLogin&dkey=XOV3IU9JU5> (last accessed on July 21, 2009).

¹⁹⁵ D. J. B. Svantesson, “How Does the Accuracy of Geo-Location Technologies Affect the Law?” *Masaryk University Journal of Law and Technology*, 2, No. 1 (Summer 2008): 11–21, at p. 12.

¹⁹⁶ Assuming that the state of Utah, which currently prohibits gambling, would continue to do so under a federal regulatory regime.

¹⁹⁷ As noted in an August 21, 2009 interview with Andrew Fritchie, General Counsel of PartyGaming PLC.

jurisdiction while gambling. Geolocation software can pinpoint the user's location and, if in doubt, flag it for site operators to either further investigate or block access immediately.

Critics of geolocation claim that it is inherently unreliable and subject to relatively easy circumvention, citing failure rates in the range of 20% to 30%.¹⁹⁸ For example, a wireless access card, a common method of accessing the Internet on a laptop while traveling, may confuse geolocation services, and each service may show the user to be in highly disparate locations.¹⁹⁹ The online gambling firm bwin uses a geolocation service, and although the company believes that the service can reliably determine the country in which a player is located, it does not currently rely on results at a state or city level.²⁰⁰ Supporters and geolocation companies themselves, however, insist that the technology is highly accurate. Quova, a market leader in geolocation technology, claimed virtually 100% accuracy in helping Ladbrokes, the world's largest bookmaker, to block Dutch users from accessing its site.²⁰¹ Other estimates of accuracy run from 85% to 99%.²⁰²

Geolocation technology is already used for a number of purposes, such as restricting access to content, protecting media rights, and delivering location-based content to users. It is used by organizations such as the New York State Lottery, the British Columbia Lottery, Major League Baseball, and the Alaska Permanent Fund.²⁰³ It is also used to detect and deter fraud at online retailers by comparing the user's location with his or her credit card address, for example, and governments and law enforcement agencies use geolocation to help track Internet criminals.²⁰⁴

Technologies to circumvent geolocation do exist, such as "overt and transparent proxies, firewalls, filters and filtering services, Network Address Translators, private address spaces, point-to-point links, tunnels, and Virtual Private Networks (VPNs), that further obfuscate the

¹⁹⁸ Statement of Jeff Schmidt, in U.S. House of Representatives, Committee on Financial Services, *Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?* 110th Cong., 1st Session, June 8, 2007, at p. 18–19.

¹⁹⁹ See *Id.*

²⁰⁰ As noted in an August 13, 2009 correspondence with Katharina Riedl of bwin (Austria).

²⁰¹ A Dutch court had ordered Ladbrokes, a U.K. bookmaker, to prevent domestic users from accessing its site. See *Supra* at footnote 194.

²⁰² See *Supra* at footnote 185 at p. 15.

²⁰³ See *Supra* at footnote 39 at p. 53. Also see Larry Barrett, "Major League Baseball Struggles to Reach Fans Online," *Baseline*, March 7, 2005, http://www.baselinemag.com/index2.php?option=content&do_pdf=1&id=3506 (last accessed on September 4, 2009). Also see Quova, *Quova Helps the Alaska Permanent Fund Dividend Division Run Like a Well-Oiled Machine*, Quova case study, 2008, https://www.vtrenz.net/imaeds/ownerassets/818/08277_Alaska_casestudy_REV2.pdf (last accessed on September 10, 2009).

²⁰⁴ Quova, *The Science of Geolocation*, <http://www.quova.com/Technology/thescienceofgeolocation.aspx> (last accessed on September 4, 2009).

true source and destination of communications.”²⁰⁵ In some cases, the user could be on a different continent from the one indicated by their IP address because he or she may be using one of the above technologies that masks the true location. VPN programs, which many people use to access work networks from home or while traveling, effectively mask one’s location. In fact, many gateways to the Internet, such as America Online or proxy servers, by their nature offer geographic separation between the IP address and the end user.²⁰⁶

Geolocation software, however, can exploit the physical characteristics of the connection, such as the round-trip delay, to detect these countermeasures and assign a “confidence factor,” indicating the probability that the reported location is the user’s actual location.²⁰⁷ Also, the software can determine if the destination address belongs to a cable company, a DSL provider, or a dial-up ISP. Thus, the destination can indicate the user’s connection type and whether it is too risky to accurately verify the user’s location.²⁰⁸ In these cases, the customer’s account can be blocked completely from using the service until his or her location can be determined with greater certainty, or the site’s compliance department can flag the account for further review. Further review could involve requiring the user to submit additional information, which then may be subject to manual or real-time verification.²⁰⁹

The regulator may impose specific requirements on the confidence of any geolocation information, on the basis of the confidence factor determined by the software, in essence to “tune” the thresholds for acceptance, rejection, and further verification.²¹⁰ For example, the New York Lottery and the British Columbia Lottery use Aristotle’s verification service for geolocation. Both organizations require nearly 100% confidence scores in order to allow users to participate in their respective lotteries.²¹¹ In this way, regulators can have as much assurance as they require in the geolocation system, making it an effective means of excluding individuals in any specific jurisdiction.

4. Conclusion

Beyond the issue of sanctions, licensed sites may have an incentive to be lax with geolocation controls: excluding users from certain states lowers their overall customer base. Therefore, a

²⁰⁵ See *Supra* at footnote 198 at p. 83.

²⁰⁶ As noted in an August 21, 2009 interview with Andrew Fritchie, General Counsel of PartyGaming PLC.

²⁰⁷ Quova, *GeoPoint by Quova*, white paper, July 2006, https://www1.vtrenz.net/imarkownerfiles/ownerassets/818/GeoPointbyQuova_WHITEPAPER.pdf (last accessed on July 21, 2009), at p. 7.

²⁰⁸ See *Supra* at footnote 194.

²⁰⁹ See *Id.*

²¹⁰ As noted in an August 3, 2009 interview with Paul Mathews, Former Senior Vice President of IGT Wagerworks. Also see *Supra* at footnote 161.

²¹¹ See *Supra* at footnote 39 at p. 53.

regulator must ensure that geolocation controls are updated frequently and meet desired standards of quality. Frequent mystery shopping at U.S. sites conducted from locations within restricted states is one option, and violators could risk losing their valuable operating license if they chose to operate lax verification techniques. This combination of oversight and state-of-the-art technology should help ensure that various jurisdictions maintain control over their own gambling laws and prevent complex interstate legal disputes.

H. Breaches of Data Confidentiality

Online gambling websites often hold personal and confidential information of their customers, including credit card and bank account numbers, names, addresses, and other sensitive information. One of the challenges for a regulator is to ensure that personal information is used only for legitimate purposes and is not disseminated or accessed improperly.

1. The Issue of Data Confidentiality

All online businesses involved in monetary transactions are susceptible to breaches of data confidentiality.²¹² Breaches can include hackers stealing credit card or other personal information, employees storing or accessing sensitive information improperly, and sites accidentally releasing personal information.²¹³ Although the deliberate theft of data is a significant problem, more than 88% of all cases of data breaches in 2008 resulted from insiders' negligence.²¹⁴ Once released, the data can then be used for various illegal purposes and may lead to identity theft and credit card fraud.

Unlike other countries, the United States does not maintain any general data privacy laws at a federal level.²¹⁵ Instead, individual states have wide latitude to enact laws protecting consumers' data, and currently 45 states have laws governing data breaches by companies.²¹⁶ Online

²¹² In January 2009, Heartland Payment Systems, the United States' fifth-largest payment processor, announced a data breach caused by hackers that may have compromised up to 100 million credit cards. TJX, a major operator of retail stores, experienced a data breach in 2006 that exposed tens of millions of cards. See Rachel King, "Lessons from the Data Breach at Heartland," *Business Week*, July 7, 2009, <http://www.msnbc.msn.com/id/31778540/ns/business-businessweekcom/> (last accessed on July 29, 2009).

²¹³ *Identity Theft Daily*, "Identity Theft News: 2008 Data Breach Count is 69% greater than 2007," *Identify Theft Daily*, <http://www.identitytheftdaily.com/index.php/20080716371/Latest/Identity-Theft-News-2008-Data-Breach-count-is-69-greater-than-2007.html> (last accessed on July 29, 2009).

²¹⁴ PGP Corporation, *2008 Annual Study: Cost of a Data Breach*, conducted by the Ponemon Institute, LLC, February 2009, at p. 5, http://www.encryptionreports.com/download/Ponemon_COB_2008_US_090201.pdf (last accessed on July 31, 2009).

²¹⁵ Dan Kaplan, "Leahy, for Third Time, Submits Federal Data Security Law," *SC Magazine*, July 24, 2009, <http://www.scmagazineus.com/Leahy-for-third-time-submits-federal-data-security-law/article/140604/> (last accessed on July 29, 2009).

²¹⁶ See *Id.* Also see National Conference of State Legislatures, *State Security Breach Notification Laws*, as of July 27, 2009, <http://www.ncsl.org/Default.aspx?TabId=13489> (last accessed on September 10, 2009).

gamblers residing in the United States currently have no protection against breaches of their personal data beyond those implemented by the online gambling site itself.

2. Existing Controls in Other Jurisdictions

In 2003, California became the first state to pass a comprehensive law on notification of data breaches. The law requires companies that experience a breach to notify all data subjects “in the most expedient time possible and without unreasonable delay” if certain types of personal information are released unintentionally. It is important to note that the data must have been unencrypted to trigger the notification.²¹⁷

A 2009 bill proposed by Senator Patrick Leahy of Vermont, dubbed the Personal Data Privacy and Security Act, aims to “require data brokers and companies to establish and implement data privacy and security programs.”²¹⁸ Leahy notes that more than 250 million records containing personal information have been breached since 2005.²¹⁹ The law would require companies that store customers’ personal data to establish internal control policies and to give notice when a breach of data occurs. The bill would preempt state laws on these matters.²²⁰ It also would establish an Office of Federal Identity Protection to assist consumers with issues of identity theft and data correction.²²¹

In Europe, most data privacy laws are highly stringent—much more so than in the United States. The European Union’s Data Protection Directive, issued in 1995, introduced strong controls on data privacy and the rights of consumers.²²² Among other provisions, it requires that data be relevant to the purpose for which it is kept, stored no longer than necessary, and verifiable by consumers. It also requires that, if data are to be processed (i.e., collected and used), (1) the data subject should have given explicit consent for its use and (2) the processing must be necessary for the performance of a contract, required by a legal obligation, necessary to protect the data subject’s life, or necessary to perform a task of public interest.

Various jurisdictions across the world that have legalized and regulated online gambling maintain rules on data confidentiality and privacy:

²¹⁷ See California Office of Privacy Protection, “Recommended Practices on Notice of Security Breach Involving Personal Information,” May 2008, http://www.oisp.pp.ca.gov/consumer_privacy/pdf/secbreach.pdf (last accessed on July 31, 2009), at p. 8.

²¹⁸ Office of Senator Patrick Leahy, *Leahy Introduces Cybersecurity Legislation*, July 22, 2009, <http://leahy.senate.gov/press/200907/072209b.html> (last accessed on July 29, 2009), at p. 1.

²¹⁹ See *Id.*

²²⁰ See *Id.* at p. 5-8.

²²¹ See *Id.* at p. 9.

²²² *Data Protection in the European Union*, European Commission, United Kingdom, http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-ukingdom_en.pdf (last accessed on September 10, 2009).

- The Isle of Man’s gambling regulations “specify detailed rules on the way accounts must be managed, privacy of information on account holders and prescribe the penalty for contravention which is £5,000 for each violation.”²²³ Site operators in the Isle of Man are also bound to the rules in the Data Protection Act 2002, the island’s legislation concerning data privacy. One of the Act’s provisions provides for compensation for “[a]n individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act.”²²⁴
- Jersey’s regulatory system requires that “[c]ustomer privacy and data protection principles are observed.”²²⁵
- Gibraltar requires that information about a player not be disclosed to a third party except under certain circumstances.²²⁶ Gibraltar’s regulator also requires that data be obtained lawfully, kept and used only for the purposes for which it was obtained, stored safely, and accessible by the customer.²²⁷

3. Relevant Technologies for Risk Mitigation

Effective data protection begins with the establishment of internal controls and policies by the gambling website. Betting site 888.com states in its privacy policy that it is “committed to respecting your privacy and to complying with applicable data protection and privacy laws and we have therefore provided this Privacy Policy to help you understand how we collect, use and safeguard your PII [personally identifiable information].”²²⁸ It also states that the site’s employees and data processors have an obligation to respect users’ privacy. Betfair’s privacy policy claims the site “endeavour[s] to ensure that [its] business practices that involve the use of...Personal Information are compliant with privacy regulations in the countries where [it] operate[s].”²²⁹ and it claims that it has assembled a “world class Information Security Management System.”

²²³ See *Supra* at footnote 30 at p. 126.

²²⁴ Data Protection Act 2002, Treasury of the Isle of Man, at §11(1).

²²⁵ See *Supra* at footnote 29 at p. 144.

²²⁶ See *Supra* at footnote 132 at §30.

²²⁷ See *Supra* at footnote 31 at p. 16.

²²⁸ See <http://www.888.com/>, under “Privacy Policy for Users” (last accessed on September 10, 2009).

²²⁹ See <http://content.betfair.com/aboutus/?product=exchange&brand=betfair®ion=GBR&locale=en> (last accessed on September 10, 2009).

Maintaining secure computer systems is a demanding task. Although the various technological solutions—secure operating systems, file encryption, network firewalls—have their weaknesses the primary failure mechanism for data security is human mistakes and carelessness.²³⁰

Absent regulation, gaming site operators would not bear many of the costs associated with the improper disclosure of personal information. Thus, a regulatory mechanism is needed to align the operator's incentives with those of consumers. A significant fine for each consumer record improperly released is one such incentive.

With the proper incentives, the gaming site operator will engage in the security engineering, training of staff, and auditing needed to protect consumer records.

4. Conclusion

In an effective regulatory regime, the regulator would require the internal controls and privacy policies described in this section to be present on gambling websites and be highly visible to customers. The regulator would ensure that employees receive training in relevant data protection policies and that players have the ability to access and, if necessary, modify their personal information. It would also establish the types of data that can be stored and the length of time after which the data must be deleted. Finally, the regulatory regime may impose criminal or civil liability on site operators whose data is breached, and it can require regular audits, either by the regulator itself or by independent third parties, of data encryption policies and other protection systems. There is no reason to believe that licensed online gambling operators would be any less able or willing to fulfill these obligations than other online merchants with similar data custody obligations. For more discussion on technological strategies to protect sites' integrity and customers' personal data, see Section I, Communications and Computer Security Failures.

I. Communications and Computer Security Failures

Security of websites, to prevent improper use of or access to sensitive data, is a ubiquitous and serious concern in e-commerce. Hackers can undermine site security, alter a site's behavior, shut it down, access customers' confidential information, or use one site as a platform from which to launch broader malicious activities across the web. Online gambling sites would be responsible, in just the same way as other merchant sites, for implementing proper controls and in cooperating with law enforcement agencies in the control of cybercrime.

1. The Issue of Communications and Computer Security Failures

Web server security can be compromised from two directions. The first is over the network (i.e. through internet connections). Second, and perhaps more importantly, a website's servers are also subject to attack or misuse by the gaming site's own employees. A key employee may be able to install software that subverts a system, destroys the integrity of games, interferes with

²³⁰ See Ross Anderson, *Security Engineering, A Guide to Building Dependable Distributed Systems* 2nd Edition, Wiley, 2008, at p. 17-62.

customer accounts, or improperly transmits customers' personal or financial information. Even an ordinary virus may render a site inoperative, making it impossible for customers to access their accounts or recover their deposits. Phishing attacks, directed at customers through a gambling website, may also be a concern.

Attacks may involve unauthorized attempts to login using someone else's account, or exploitation of some security weakness in the web server software itself or in the communications software on the server.²³¹

Protecting gaming websites from intruders is little different from the problem faced by government agencies or online merchants such as Amazon. Many organizations do this quite well as a matter of course, and licensed gambling site operators should be held to a high standard.

There are currently no U.S. federal laws regarding data breaches, and the issue is left to individual states. However, acts of hacking and computer fraud are addressed by the Computer Fraud and Abuse Act, originally enacted in 1986, which covers any interstate or international computer communications.²³² The Act criminalizes a wide range of computer fraud, including improperly accessing a "protected" computer with intent to defraud and knowingly transmitting a program or code that causes damage to multiple computers. A 2008 amendment to the law eliminated the requirement for the communications to be interstate or international in cases involving theft and broadened the definition of a "protected computer" to mean any computer used in interstate or foreign communication.

Like other heavily-used websites, gambling sites are susceptible to denial-of-service attacks, which overload a website's servers and force it to shut down.²³³ The threat of such attacks has been used to extort money from website operators. Perpetrators of such extortion have included organized crime groups from the Middle East and Asia.²³⁴ In 2004, British bookmakers alone lost \$70 million due to "cyber-extortion" by just one hacking team, and companies such as

²³¹ For a description of a recent (September 2009) discovery of a security weakness in web server software, see Gregg Keizer, *Microsoft promises patch for critical Web server bug*, Computerworld, September 2, 2009, http://www.computerworld.com/s/article/9137438/Microsoft_promises_patch_for_critical_Web_server_bug (last accessed on September 9, 2009).

²³² See U.S. Department of Justice, *Chapter 1 – Computer Fraud and Abuse Act*, Computer Crime & Intellectual Property Section, <http://www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.pdf> (last accessed on July 29, 2009).

²³³ Denial-of-service attacks use computers to inundate a website with large amounts of internet traffic that eventually slows the site or shuts it down completely. See Jack M. Germain, "Global Extortion: Online Gambling and Organized Hacking," *Tech News World*, March 23, 2004, <http://www.technewsworld.com/story/33171.html?wlc=1248627730> (last accessed on July 26, 2009). Also see Jordan Robertson, "Tech 101: How a Denial-of-Service Attack Works," *Associated Press*, July 8, 2009, <http://www.usnews.com/articles/science/2009/07/08/tech-101-how-a-denial-of-service-attack-works.html?PageNr=1> (last accessed on July 28, 2009).

²³⁴ See *Id.*

Canbet, Harrods Casino, Inter Casino Poker, Totalbet, VIP Casino, and William Hill have been the victims of denial-of-service attacks.²³⁵

Users of gambling websites are also susceptible to phishing, or the use of fraudulent but credible-looking website-mimics to deceive the user into releasing personal information or to install viruses and other malware onto their computers.²³⁶ Phishing may take many forms including fraudulent or misleading email, website pop-up advertisements, or other forms of electronic communication such as text messaging. Phishing attacks cost consumers more than \$3 billion annually in the form of fraudulent credit card charges, withdrawals from compromised bank accounts, time spent rectifying fraud problems, and reduced trust in online commerce.²³⁷ Depending upon factors such as the website's payout policy or the ability to transfer funds between players, gambling websites can be attractive targets for phishing.²³⁸

2. Existing Controls in Other Jurisdictions

In a licensed regulatory environment, gambling site operators would be expected to play their part—just like any other e-commerce merchant—in eliminating their own security vulnerabilities and cooperating with law-enforcement agencies in cybercrime control. Existing U.S. laws (federal and state) regarding computer intrusion would apply, and sites would have recourse to law enforcement support if they suffered attacks. Other nations have legal regimes similar to the U.S. with respect to cybercrime. France, Germany, and the United Kingdom all have laws specifically targeting cybercrime, and the European Union is currently looking to both strengthen its laws on cybersecurity and harmonize the laws of its member states.²³⁹ The European Union is also considering a system through which members can report Internet-based attacks to each other and record arrests and prosecutions.²⁴⁰ The Licensing, Regulation, and Alcohol Strategy division

²³⁵ See John McMullan and Aunshul Rege, *Cheating and Cybercrimes @ Gambling Sites.com*, presentation to the Alberta Gambling Research Institute Annual Conference, March 2009, slide 17. Also see John McMullan and David Perrier, "The Security of Gambling and Gambling with Security: Hacking, Law Enforcement and Public Policy," *International Gambling Studies* 7, No. 1 (2007): 43–58 at p. 47.

²³⁶ Rachna Dhamija *et al.*, *Why Phishing Works*, Experimental Social Science Laboratory (Xlab), Paper XL06-013 (August 14, 2006): 581–590 at p. 581, <http://repositories.cdlib.org/iber/xlab/XL06-013> (last accessed on August 3, 2009). Also see Cyveillance, *The Cost of Phishing: Understanding the True Cost Dynamics Behind Phishing Attacks*, white paper, December 2008, http://www.cyveillance.com/web/docs/WP_CostofPhishing.pdf (last accessed on August 3, 2009). Also see APWG, *Phishing Activity Trends Report Q1/2008*, January–March 2008, http://www.antiphishing.org/reports/apwg_report_Q1_2008.pdf (last accessed on August 3, 2009).

²³⁷ See *Id* Cyveillance.

²³⁸ Marvin Fabuli, "Online Casinos an Easy Bet for Phishers," Symantec, February 27, 2008, <http://www.symantec.com/connect/blogs/online-casinos-easy-bet-phishers> (last accessed on August 3, 2009).

²³⁹ Palmer, Maija, "EU plans tougher cybercrime laws," *FT.com*, June 14, 2009, <http://www.ft.com/cms/s/0/10a407b6-5913-11de-80b3-00144feabdc0.html> (last accessed on August 2, 2009).

²⁴⁰ See *Id*.

in Australia's Northern Territory requires license applicants to submit their information technology security protocols for a risk assessment, and their controls must adhere to Australian and New Zealand AS/NZS 4444 standards for information security.²⁴¹

The issue of hacking is not completely unfamiliar to bricks-and-mortar casinos. They use quite sophisticated electronic systems, which are vulnerable as well.²⁴² A regulatory strategy for online gambling would require implementation and maintenance of state-of-the-art security controls, cooperation with law-enforcement on cybercrime issues, comprehensive testing of site and account security for the sake of defending consumers' privacy and interests, and mandatory reporting of any attacks.²⁴³

3. Relevant Technologies for Risk Mitigation

The key technologies for gambling website security are the same as those used by other on-line merchants. These include (1) network firewalls that isolate databases, administrative systems, and development systems from the Internet, (2) high-quality servers with up-to-date security patches, (3) a continuing process of monitoring and logging attempts to break into the system over the Internet, (4) secure database and transactional software, and (5) the use of secure, encrypted protocols for communications between users and the gambling website.²⁴⁴

Intruders who gain access to a user's credentials and use those credentials to open a fraudulent connection can be combated in several ways. Many gambling sites work by having users download and install dedicated client software to access the site rather than relying on standard web browsers. This dedicated client software can implement security protocols that resist a variety of exploits such as keystroke loggers and "man-in-the-middle" attacks.²⁴⁵ For example, the gambling site could use encryption keys based, in part, on information exchanged at registration and stored on the user's computer. This approach, however, is not as user friendly as a simple login (e.g., user name and password), as it would make the use of any computer other than the user's regular computer more difficult.

²⁴¹ As noted in an August 31, 2009 correspondence with John Sealy, Manager of Information Systems and Technology Services at the Licensing, Regulation and Alcohol Strategy division of the Northern Territory Department of Justice (Australia).

²⁴² See John McMullan and David Perrier, "The Security of Gambling and Gambling with Security: Hacking, Law Enforcement and Public Policy," *International Gambling Studies* 7, No. 1 (2007): 43-58 at p. 44.

²⁴³ See *Id.* at p. 53.

²⁴⁴ Keys Botzum, WebSphere Application Server V6 advanced security hardening -- Part 1, Overview and approach to security hardening, IBM WebSphere Developer Technical Journal, December 2005, http://www.ibm.com/developerworks/websphere/techjournal/0512_botzum/0512_botzum1.html (last accessed on September 14, 2009)

²⁴⁵ Keystroke loggers are programs that record users' keystrokes for the purpose of garnering private information such as passwords. "Man-in-the-middle" attacks are cryptographic attacks in which an eavesdropper relays messages between two victims. The eavesdropper can read and even alter the messages.

Another approach is to add a feature to the user's password. It is common for high-value websites to put an additional password on a physical device, such as a small keyfob that displays a six-digit number that changes once per minute.²⁴⁶ The user logs in by supplying the user name, password, and the number on the fob, and these are passed through to the server, which authenticates them and permits the user to log in. This technology protects against lost and easy-to-guess passwords but not against man-in-the-middle attacks. However, if the site requires the user to employ dedicated client software, that client software can use the 6-digit number as part of the encryption key for establishing the connection between the user's computer and the web server; this technique would successfully protect against man-in-the-middle attacks.²⁴⁷

Gambling site operators are already aware of some of these options. For example, PartyGaming's privacy policy states that it stores all players' personal information in a password-protected database behind a state-of-the-art firewall, and the site itself supports SSL version 3 security with 128-bit encryption.²⁴⁸ It also states that it ensures that affiliates, subsidiaries, agents, and suppliers use secure technology. The site 888.com claims that it uses advanced SSL and PGP protocols for security along with public/private key encryption and firewalls.²⁴⁹ Both sites employ secure, dedicated client software. Other gambling sites also enumerate details about their security policies and procedures, all of which are designed to prevent unauthorized access to personal information.

Denial-of-service attacks present a particular challenge to gaming site operators. The harmful traffic usually arises from thousands or tens of thousands of computers that have been infected with a virus that permits the author of the virus to remotely control the infected computer. The individual commanding such a network can direct the entire network to begin loading pages from the gambling website. If the website is designed to serve a thousand active users but ten thousand computers begin loading web pages at ten times the rate of a normal user, service from the website could collapse.

Some technological countermeasures are available to the website operator—for example the website could place limits on the number of new computers from which it will accept connections. However, if the flow of incoming traffic is big enough it will overload the connections between the gambling site and the rest of the Internet. Thus, the ultimate control of denial-of-service attacks must come from web administrators, providers of operating system software, and network service providers.

²⁴⁶ This process is called two-factor authentication. One factor is the normal password which the user types, and the other is the code from the key fob. The interactive role-playing game service World of Warcraft provides such key fobs to its users for a fee of \$6.50. See <http://www.blizzard.com/store/details.xml?id=1100000622> (last accessed on September 9, 2009).

²⁴⁷ If the 6-digits are used as a shared secret to generate part or all of the encryption key for the communications between the user and the game site, then a man-in-the-middle attack is impossible because the attacker lacks the shared secret.

²⁴⁸ See https://secure.partyaccount.com/about/privacy_s.do (last accessed on August 24, 2009).

²⁴⁹ See <http://www.888.com/> (last accessed on August 24, 2009).

Security failures in computer operating systems are the gateway through which most viruses infect computers. Network service providers have the ability to monitor traffic flows on many different paths and can detect patterns of activity that indicate the beginnings of a denial-of-service attack. They may also be able to control denial-of-service attacks at locations far from the connection to the gambling site.

For this reason, sites must work closely with regulators and government agencies to identify and deal with cybercriminals. Regulators should develop cooperative relationships with private security experts and advocate for cost-effective, industry-wide benchmarks for cyber-security.²⁵⁰ Finally, legislators should consider imposing civil liability on site operators for any harm caused by computer intrusions, at least when site security precautions were not up to the requisite standard.²⁵¹

Finally, gambling site operators, like all other online merchants, should implement anti-phishing measures to prevent financial harm to consumers and maintain the integrity of their operations. The sites should play their role in helping to educate consumers about safe browsing habits and how to recognize phishing.²⁵²

4. Conclusion

Significant international attention is already being paid to cybercrime in general. Website security is a matter of global concern for businesses and government alike, by no means specific to online gambling. According to a Cyberspace Policy Review report released in 2009 by the Cybersecurity Chief at the National Security Council, “a growing array of state and non-state actors are compromising, stealing, changing, or destroying information and could cause critical disruptions to U.S. systems.”²⁵³ The report recommends a coordinated effort by federal, state, and local governments along with security experts in the private sector, and it urges the government to “identify procurement strategies that will incentivize the market to make more secure products and services available to the public.”²⁵⁴ It goes on to recommend “adjustments to liability considerations (reduced liability in exchange for improved security or increased

²⁵⁰ See John McMullan and Aunshul Rege, *Cheating and Cybercrimes @ Gambling Sites.com*, presentation to the Alberta Gambling Research Institute Annual Conference, March 2009, slide 23.

²⁵¹ John McMullan and David Perrier, “The Security of Gambling and Gambling with Security: Hacking, Law Enforcement and Public Policy,” *International Gambling Studies* 7, No. 1 (2007): 43–58 at p. 56.

²⁵² MarkMonitor, “Rock Phishing: The Threat and Recommended Countermeasures,” White Paper, August 2007, <http://www.markmonitor.com/download/wp/wp-rockphish.pdf> (last accessed on August 3, 2009), at p. 7–8.

²⁵³ Cyberspace Policy Review, *Assuring a Trusted and Resilient Information and Communications Infrastructure*, National Security Council, May 2009, <http://www.whitehouse.gov/asset.aspx?AssetId=1906> (last accessed on August 2, 2009), p. iii. Also see <http://www.whitehouse.gov/cyberreview/>.

²⁵⁴ See *Id* at p. iv-v.

liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms.”²⁵⁵

While all online merchants would benefit from increased governmental and law enforcement support, online gambling operators are ultimately responsible for their own sites’ security. Site operators will naturally be concerned with their reputations for integrity and reliability, but regulation can introduce new incentives to ensure that operators deploy effective security. The regulator might choose to mandate some specific technologies, such as SSL encryption and dedicated client software; and it can sharpen the incentives for effective control by imposing higher levels of liability for any sites that fail to implement adequate precautions.

J. Problem Gambling

1. Problem Gambling

We expect that problem gambling behaviors may receive more attention in the upcoming debates than any of the other categories of risk. Therefore, we discuss problem gambling in more detail in Section III below.

²⁵⁵ See *Id* at p. v.

III. SPECIAL ATTENTION TO PROBLEM GAMBLING

A. Introduction

Unlike the other nine risks, the potential effect of legalization on problem gambling is less obvious a priori. On the one hand, in a well-regulated online environment, gamblers (including existing U.S.-based online gamblers) would have more access to mechanisms with which to try to curb their problem behavior. These include tools for self-exclusion and self-limits as well as greater awareness of and access to clinical and self-help resources. On the other hand, pathological or addictive gambling behaviors might nevertheless be exacerbated by the increased opportunity to gamble at any time and from anywhere.

B. What is Problem Gambling?

1. Terminology

Problem gambling is a term without a specific definition that refers to the fact that some individuals who gamble do so irresponsibly and damage or disrupt personal, financial, or social pursuits.²⁵⁶ The term can apply to a wide spectrum of cases, from less severe ones where individuals experience some degree of gambling-related problems to more severe cases in which individuals are clinically diagnosed with *pathological gambling*—an impulse control disorder.²⁵⁷

²⁵⁶ Lack of specific definition noted in an August 5, 2009 interview with Phill Brear, Head of Gambling Regulation at the Gibraltar Regulatory Authority. National Council on Problem Gambling, *FAQs – Problem Gamblers*, <http://www.ncpgambling.org/i4a/pages/Index.cfm?pageID=3315> (last accessed on July 11, 2009).

²⁵⁷ In 1980, the American Psychiatric Association (APA) first included pathological gambling in the Diagnostic and Statistical Manual for Mental Disorders (DSM). It was described as a “chronic and progressive failure to resist impulses to gamble, characterized by undesirable outcomes ranging from borrowing money from family or friends and losing time at work, to being arrested for offenses committed to support gambling.” National Research Council, *Pathological Gambling: A Critical Review*, Washington, DC: National Academy Press (2005), at p. 2. In the most current manual, DSM-IV, the APA lists 10 diagnostic criteria of which five have to be met to make a clinical diagnosis of pathological gambling. See *Id* at p. 27. Various screening mechanisms have been developed to assess levels of problem gambling, including the South Oaks Gambling Screen (SOGS), the Problem Gambling Severity Index (PGSI) of the Canadian Problem Gambling Index (CPGI), and the National Opinion Research Center DSM Screen for Gambling Problems (NODS). See Michael Belletire *et al.*, *Legislating and Regulating Casino Gaming: A View from State Regulators*, paper commissioned by the Regulation, Enforcement and Internet Subcommittee of the National Gambling Impact Study Commission, 1999, at p. 11. Also noted in interviews with Peter Collins, Professor of Public Policy Studies and Director of the Center for the Study of Gambling at the University of Salford (U.K.), and Sam McQuade, Graduate Program Coordinator at the College of Applied Science and Technology at the Rochester Institute of Technology.

2. Prevalence Rates and Trends

Worldwide: Most research indicates that about 1% of the adult population worldwide experiences severe problem gambling.²⁵⁸ Moreover, studies indicate that severe problem gambling rates globally have stabilized over time at about 1%.²⁵⁹

United States: Various studies have been conducted to estimate the prevalence of problem gambling in the United States. According to the National Council on Problem Gambling, about 1% of the U.S. adult population meets the criteria for pathological gambling in a given year. Another 2% to 3% would be considered problem gamblers.²⁶⁰ In a meta-analysis of 120 previously conducted prevalence studies in the United States and Canada, researchers at the Division of Addictions at Harvard Medical School derived point-in-time estimates of problem gambling rates. They noted that 1% to 2% of the adult population met criteria for lifetime pathological gambling.²⁶¹ A more recent estimate from a nationally representative survey in the United States found lifetime pathological gambling rates within the general population of 0.4%.²⁶² In an interview in mid 2009, Howard J. Shaffer, an addiction expert at Harvard University, noted that despite the substantial growth in gambling opportunities and overall gambling volume over the last two decades in the United States, the rate of problem gambling among the adult population has stayed roughly constant. Shaffer also stated that the incidence of problem gambling in the United States had declined slightly since the 1970s, from 0.7% to 0.6%.²⁶³

Online Gambling and the Incidence of Problem Gambling: Some studies have claimed an association between increased gambling exposure and increased incidence of problem

²⁵⁸ Jamie Wiebe *et al.*, *Problem Gambling Prevalence Research: A Critical Overview*, a report to the Canadian Gaming Association, December 2007, at p. 2, http://canadiangamingassociation.com/media_uploads/pdf/78.pdf (last accessed on September 10, 2009).

²⁵⁹ See *Id.* Also see D. A. LaPlante and H. J. Shaffer, “Understanding the Influence of Gambling Opportunities: Expanding Exposure Models to Include Adaptation,” *American Journal of Orthopsychiatry*, 77, No. 4 (2007): 616–623 at p. 619.

²⁶⁰ See *Supra* at footnote 256. Also noted in a June 5, 2009 interview with Keith Whyte, Executive Director of the National Council on Problem Gambling.

²⁶¹ Howard Shaffer *et al.*, “Updating and Refining Prevalence Estimates of Disordered Gambling Behaviour in the United States and Canada,” *Canadian Journal of Public Health*, 92, No. 3 (2001): 168–172 at p. 169. Also see Howard Shaffer *et al.*, *Estimating the Prevalence of Disordered Gambling Behavior in the United States and Canada: A Meta-Analysis*, Boston: Presidents and Fellows of Harvard College, 1997, at p. iii. Also see Howard Shaffer *et al.*, “Estimating the Prevalence of Disordered Gambling Behavior in the United States and Canada: A Research Synthesis,” *American Journal of Public Health*, 89, No. 9 (1999): 1369–1376 at p. 1370.

²⁶² N. M. Petry *et al.*, “Comorbidity of DSM-IV pathological Gambling and Other Psychiatric Disorders: Results from the National Epidemiologic Survey on Alcohol and Related Conditions,” *Journal of Clinical Psychiatry*, 66, No. 5 (2005): 564–574 at p. 564.

²⁶³ As noted in a June 10, 2009 interview with Howard Shaffer, Director of the Division on Addictions and Associate Professor of Psychology in the Department of Psychiatry at the Cambridge Health Alliance.

gambling.²⁶⁴ In addition, commentators have suggested that the increased accessibility inherent in online gambling magnifies such risks.²⁶⁵ However, more recent studies specific to online gambling, most conducted since the advent of legal and regulated online gambling, have indicated that online gambling does not inherently encourage excessive gambling.²⁶⁶ For example, researchers at Harvard Medical School studied real-time betting activities of 48,000 Internet players over two years and found that their betting levels in Internet sports gambling and casino games were moderate. Most gamblers placed fewer than four bets per day, and sports gamblers tended to moderate their play based on their wins and losses; i.e., they played less often when they lost money and more often when they won money.²⁶⁷ Also, a large-scale British study in 2007 found no increase in the rate of problem gambling in the United Kingdom since 1999, despite a large increase in the number of new gambling opportunities (although the number of people who had gambled in the past year decreased between 1999 and 2007).²⁶⁸

C. Potential Effects of Legalization of Online Gambling on Problem Gambling

Some researchers and policymakers have expressed concerns about the impact of online gambling on problem gambling.²⁶⁹ They fear that legalization of online gambling might spur excessive gambling and problem gambling incidence by facilitating (1) unlimited access and availability of gambling platforms; (2) anonymity, which would allow gamblers to participate without fear of stigma; (3) gambling under the influence; (4) decreased perception of value of

²⁶⁴ See Brian Rush *et al.*, “Mapping the Prevalence of Problem Gambling and Its Association with Treatment Accessibility and Proximity to Gambling Venues,” *Journal of Gambling Issues*, 20 (2007): 193–214.

²⁶⁵ As noted in interviews with Howard Shaffer, Director of the Division on Addictions and Associate Professor of Psychology in the Department of Psychiatry at the Cambridge Health Alliance, and Simon Holliday, Director of H2 Gambling Capital (U.K.).

²⁶⁶ Richard LaBrie *et al.*, “Assessing the Playing Field: A Prospective Longitudinal Study of Internet Sports Gambling Behavior,” *Journal of Gambling Studies*, 23, No. 3 (2007): 231–243. Also see Richard LaBrie *et al.*, “Inside the Virtual Casino: A Prospective Longitudinal Study of Actual Internet Casino Gambling,” *European Journal of Public Health*, 18, No. 4 (2008): 410–416. Also see Debi LaPlante *et al.*, “Sitting at the Virtual Poker Table: A Prospective Epidemiological Study of Actual Internet Poker Gambling Behavior,” *Computers in Human Behavior*, 25, No. 3 (2009): 711–717.

²⁶⁷ See “Real-Time Betting Analysis of Internet Casino Gambling,” *Responsible Gaming Quarterly*, 6, No. 2 (Fall 2008), at p. 9, http://www.americangaming.org/assets/files/RGQ_Fall_08.pdf (last accessed on August 10, 2009). Also, as noted in interviews with Peter Collins, Professor of Public Policy Studies and Director of the Center for the Study of Gambling at the University of Salford (U.K.), Bo Bernhard, Director of Gambling Research at the UNLV College of Hotel Administration, and Charles Wellford, Professor of Criminology and Criminal Justice at the University of Maryland, College Park, the availability of new forms of gambling does not necessarily lead to increased incidence of problem gambling.

²⁶⁸ See *Supra* at footnote 12, Heather Wardle *et al.* at p. 9-10.

²⁶⁹ Martin Owens and Guy C. Clark, “Internet Gambling Deserves a New Chance,” *The Debate Room*, *Businessweek*, 2007, http://www.businessweek.com/debateroom/archives/2007/09/internet_gambli.html (last accessed on September 10, 2009). Also see Michael P. Scharf and Melanie K. Corrin, “On Dangerous Ground: Passive Personality Jurisdiction and the Prohibition of Internet Gambling,” *New England Journal of International and Comparative Law*, 8, No. 1 (2002).

money; and (5) isolation.²⁷⁰ A notable example of this concern is the 1999 assertion by the National Gambling Impact Study Commission that the three main reasons to prohibit online gambling are abuse by underage gamblers, addiction by pathological gamblers due to its high speed and instant gratification, and the potential for criminal activities.²⁷¹ Policymakers are also concerned about negative spillovers to the rest of society, including increases in crime, lost work and school hours, and increase in personal debt. However, the only reason cited in the Safe Port Act (the sponsoring legislation of the UIGEA) for banning financial transactions to and from online gambling sites is that it leads to debt collection problems for U.S. financial institutions.²⁷²

The following sections describe and analyze mechanisms through which legalization could affect the level of problem gambling in the United States. We identify several mechanisms by which legalization is commonly expected to increase the incidence of problem gambling and two mechanisms by which regulation might be expected to alleviate problem gambling.

1. Potential Adverse Effects of Legalization

The following section describes several mechanisms by which legalization is commonly expected to increase the incidence of problem gambling.

a. *Removal of Legal Deterrence*

Potential Effect: It is commonly believed that current legal restrictions on online gambling have deterred would-be gamblers from engaging in the Internet's version of gambling. Therefore, legalization may accentuate problem gambling by eliminating any legal inhibitions would-be gamblers have toward online gambling. In the 2007 UNLV survey of Nevadans, researchers found that approximately 12% of "non-online gamblers" (defined as those respondents who had not gambled online, but who may or may not have otherwise gambled) would be more likely to participate in online gambling if it were licensed and regulated by the state of Nevada.²⁷³

²⁷⁰ See *Id* Scharf and Corrin. Also see *Supra* at footnote 24 at p. 50. Also Griffiths notes that among other factors, increased access to gambling provided by online gambling might facilitate the development of gambling related issues. M. D. Griffiths, "Internet Gambling: Issues, Concerns and Recommendations," *Cyberpsychology & Behavior*, 6, No. 6 (2003): 557–568; cited by Sarah E. Nelson *et al.*, "Real Limits in the Virtual World: Self-Limiting Behavior of Internet Gamblers," *Journal of Gambling Studies*, 24 (2008): 463–477, DOI 10.1007/s10899-008-9106-8. Also The Committee on the Social and Economic Impact of Pathological Gambling notes that "More people are gambling, and they are wagering more. As a result, there is increased concern about pathological gambling." The Committee further notes that "With the increased availability of gambling and new gambling technologies, pathological gambling has the potential to become even more widespread." National Research Council, *Pathological Gambling: A Critical Review* (National Academy Press, Washington, DC, 2005), at p. 3.

²⁷¹ *National Gambling Impact Study Commission, Final Report*, 1999, at p. 5-4 to 5-6, <http://govinfo.library.unt.edu/ngisc/reports/finrpt.html> (last accessed on September 10, 2009).

²⁷² See *Supra* at footnote 68 at p. 62.

²⁷³ See *Supra* at footnote 5 Bo Bernhard at p. 25, 46. Note $N = 1,000$. Also 96.3% of responders were non-online gamblers; that is, they stated that they had not gambled online in the last five years.

Mitigating Considerations: It can be argued that the lifting of the prohibition itself is unlikely to have any significant impact on would-be gamblers' willingness to gamble online, because gamblers in the United States are generally ignorant or completely confused about existing legal restrictions.²⁷⁴ Support for this argument is found in the survey mentioned above, in which researchers discovered that 53.7% of responders were unclear regarding the legal status of online gambling. Approximately 17% thought online gambling was legal, and the remaining 29.5% thought it was illegal.²⁷⁵ This result indicates general confusion among gamblers in the United States about current legal restrictions.²⁷⁶ In addition, 87.9% of the responders noted that the current legal status of online gambling did not affect their desire to gamble online, whereas 4% indicated that their desire to gamble online was very much affected by its current legal status.

Moreover, the absence of any enforcement against online gamblers until very recently may have diluted the deterrent effect of legal restrictions on would-be gamblers' inclination to gamble, leading one to argue that complete removal of such restrictions in the future would not have a major impact on the behavior of would-be gamblers.²⁷⁷

b. *Introduction of Trustworthy Brands*

Potential Effect: Legalization may lead to increased comfort with gambling online, because U.S.-based sites, with trusted brands and subject to strict regulation, would offer a range of protections to gamblers that many offshore sites do not.²⁷⁸ Moreover, greater competition in the sector, with gambling platforms offering better deals to would-be gamblers, might lead to increased volumes and greater incidence of problem gambling.

Researchers indicate that security concerns and legitimacy are two main reasons cited by gamblers for not gambling online.²⁷⁹ Currently, Online Casino City, a guide to online gambling websites, lists 1,906 gambling websites from 70 different jurisdictions, 42 of which have sites

²⁷⁴ As noted in a June 5, 2009 interview with Keith Whyte, Executive Director of the National Council on Problem Gambling, Americans are generally ignorant of the legal status of online gambling, and many do not believe they will be prosecuted for gambling online.

²⁷⁵ Researchers further noted that 54% of non-online gamblers were unclear about the current status of online gambling, whereas 16% deemed it legal and the remaining 29% deemed it illegal. ²⁷⁵ See *Supra* at footnote 5 Bo Bernhard at p. 26.

²⁷⁶ Gaul notes that "even as bettors around the world gamble millions of dollars online, confusion reigns about the legal status of those bets and the companies that handle them." See *Supra* at footnote 82. Also, in a June 10, 2009 interview, Bo Bernhard, Director of Gambling Research at the UNLV College of Hotel Administration noted that the legal status of online gambling is "very unclear" in people's minds in the United States.

²⁷⁷ See *Supra* at footnote 13.

²⁷⁸ Section 2b discusses responsible gambling practices and safeguards that may be offered by regulated online gambling websites.

²⁷⁹ See *Supra* at footnote 18, Sally Monaghan.

that allow players from the United States.²⁸⁰ The majority of these websites are privately owned, and many are located in countries with no reporting requirements.²⁸¹

In such situations, where consumers are uncertain and have limited experiences with providers, brand associations are known to be particularly influential.²⁸² In a recent survey, researchers at the University of Lethbridge found that the general reputation of the website was the most common reason identified by online gamblers for choosing to gamble at one Internet site over another.²⁸³ Thus, the introduction of branded providers that are inherently perceived to be trustworthy might attract more gamblers to participate in online gambling.²⁸⁴

Mitigating Considerations: It can be argued that gamblers most likely to be influenced by the availability of trusted brand-name sites are those who gamble already, perhaps in the casino environment, and hence know the brands.²⁸⁵ Although these gamblers may indeed shift their business, this shift would represent displacement, not overall growth. Further, the displacement would be from bricks-and-mortar to online gambling, which can offer more options and protections for problem gamblers than can land-based casinos.²⁸⁶

²⁸⁰ As of September 14, 2009. See Online Casino City, *Online Gaming Site Owners*, <http://online.casinocity.com/ownership>. Also note, amongst these 1,906 sites are included 34 sites based in the United States, most of which involve skill games, free poker tournaments in which players can win real money, or state-sponsored lottery or sports betting.

²⁸¹ Gaul notes that in a joint investigation, the *Washington Post* and CBS's *60 Minutes* found that "many Internet gambling sites operate in a shadowy world of little regulation and even less enforcement," See *Supra* at footnote 82.

²⁸² Stevie Watson *et al.*, "The Legalization of Internet Gambling: A Consumer Protection Perspective," *Journal of Public Policy & Marketing*, 23, No. 2 (2004): 209–213, at p. 211.

²⁸³ Robert Wood and Robert Williams conducted two surveys. The first survey was a random digit dial telephone survey of 8,498 Canadian adults conducted from January 2006 to June 2007. The second survey was an online self-administered survey of 12,521 adults from 105 countries, conducted from June to December 2007. See Robert Wood and Robert Williams, *Internet Gambling in Comparative Perspective: Patterns, Problems, and Interventions*, University of Lethbridge, Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

²⁸⁴ As noted in an August 4, 2009 interview with Simon Holliday, Director of H2 Gambling Capital (U.K.), the legalization of online gambling would probably increase the number of online gamblers. Also, the previously cited UNLV study revealed that 12% of non-online gamblers would be more likely to participate in online gambling if it were licensed and regulated by Nevada. Although some of these respondents may fear legal repercussions, some may be unwilling to gamble online due to a lack of credible, branded providers, because a large portion of respondents had doubts about the integrity of online gambling. See *Supra* at footnote 72.

²⁸⁵ MGM Mirage, a large U.S. bricks-and-mortar casino operator, set up an Internet gambling site based in the Isle of Man and marketed the site using MGM's brand name and credibility. See Richard McGowan, *The Gambling Debate* (Westport, CT: Greenwood Press, 2008), at p. 43.

²⁸⁶ Wiebe and Lipton note that "If players value such regulation, then the unregulated operators will be at a competitive disadvantage." Jamie Wiebe and Michael Lipton, *An Overview of Internet Gambling Regulations*, submitted to the Ontario Problem Gambling Research Centre, August 2008, at p. 15.

c. *Increased Accessibility*

Potential Effect: One of the most common critiques of online gambling is the increase in access and availability inherent in Internet-based gambling platforms.²⁸⁷ Many believe that increased access to gambling and 24-hour-a-day availability may exacerbate problem gambling.²⁸⁸ In addition, online gambling also facilitates (1) anonymity, allowing gamblers to participate without fear of stigma; (2) gambling under the influence; and (3) decreased perception of the value of money, thereby elevating the risks of problem gambling. Potential risks posed by the frequency and speed of gaming, variety of games, and smaller permissible bet size on the Internet are frequently cited.²⁸⁹

Mitigating Considerations: U.S. residents already have online gambling options available to them all day, everyday, and from anywhere. So the addition of U.S.-licensed sites would not alter that particular reality.²⁹⁰ Furthermore, as discussed in Section 2b below, regulation can assuage these concerns. Responsible gaming features and safeguards, including links to problem gambling help-lines and websites, self-exclusion programs, and self-imposed time and money limits, are some common features that can be enforced to curb problem gambling. In fact, some have suggested that problem gamblers may benefit the most from the legalization of online gambling, because they would gain access to the tools required by the regulator.²⁹¹

d. *Easier Flow of Funds if UIGEA Restrictions are Lifted*

Potential Effect: Absent UIGEA restriction, U.S. residents would be able to make deposits to and withdrawals from online sites with greater ease. The UIGEA was intended to stop the transfer of funds from U.S. gamblers to online gambling websites. Instead of criminalizing gambling itself, the UIGEA was intended to prevent U.S. residents from gambling by restricting the role of financial institutions in transmitting payments to and from gaming operators.

Mitigating Considerations: Currently, enough workarounds have been designed, and are actively promoted to consumers by offshore online gambling sites, to render the existing restrictions largely ineffective. U.S. gamblers primarily use services provided by offshore financial intermediaries unrelated to gambling sites, such as e-wallets, that allow customers to get around the restrictions placed by the UIGEA. An e-wallet is an online account in which money can be deposited and used in commercial transactions. The e-wallet draws on a consumer's bank or

²⁸⁷ See *Supra* at footnote 68 at p. 61. Also noted in August 7, 2009 interview with Jamie Wiebe, Director at the Centre for the Advancement of Best Practices of the Ontario Responsible Gambling Council.

²⁸⁸ Michael Smeaton and Mark Griffiths, "Internet Gambling and Social Responsibility: An Exploratory Study," *CyberPsychology & Behavior*, 7, No. 1 (2004): 49–57, at p. 50.

²⁸⁹ See *Supra* at footnote 68 at p. 61.

²⁹⁰ See *Supra* at footnote 152 at p. 15.

²⁹¹ As noted in an August 27, 2009 interview with André Wilsenach, Chief Executive Officer of the Alderney Gambling Control Commission.

credit card and routes the funds to the merchant, in this case an online gambling website. The most widely used e-wallets facilitate billions of dollars in commerce annually and are based and regulated offshore.²⁹²

The UIGEA restrictions have not produced the intended deterrence to online gambling and may have unintentionally led to the surfeit of unregulated offshore intermediaries, which act as alternatives to regulated U.S.-domiciled financial institutions. Removal of these restrictions is therefore expected to have limited impact on the incidence of problem gambling.

In addition, as discussed in Section E, legalization would give regulators an opportunity to gain better oversight on such international money transfers when routed through regulated financial institutions. It would also provide consumers with the protections already available to credit card holders in the event of fraud, disputes, and complaints.

e. *Advertising*

Potential Effect: Currently, the U.S. Department of Justice (DOJ) has the authority to prohibit the advertising of illegal Internet gambling websites. In 2003, the DOJ issued letters to the National Association of Broadcasters and other media groups noting that allowing advertising for online gambling websites may be considered aiding or abetting illegal gambling operations.²⁹³ Legalization of online gambling may, however, facilitate resumption of advertising in support of the online business.²⁹⁴

The high level of exposure to land- and river-based gambling and state lottery advertisements has contributed to gambling's normalization and perception as an ordinary and harmless activity.²⁹⁵ Various marketing strategies, including pop-up promotions, free or practice games, and direct email campaigns, are already being used to promote online gambling.²⁹⁶ Some advocates suggest that such advertising could lure would-be and existing gamblers to participate in online gambling, thereby leading to greater incidence of problem gambling.²⁹⁷

²⁹² Todd notes that the UIGEA does not seem to have had an impact on online gambling in the United States. Aaron Todd, *NETeller Exit Impacts U.S. Internet Gambling Market*, onlineCasinoCity, Jan. 18, 2007, <http://online.casinocity.com/news/news.cfm?ArticleId=70015> (last accessed on September 11, 2009); cited by Gerd Alexander, "The U.S. on Tilt: Why the Unlawful Internet Gambling Enforcement Act is a Bad Bet," *Duke Law & Technology Review*, 5 (2008), at ¶6.

²⁹³ See *Supra* at footnote 59 at ¶11–12.

²⁹⁴ It should be noted, however, that the FTC and the various state attorneys general would in all likelihood retain jurisdiction over advertising online and the FCC would retain jurisdiction over advertising on broadcast and cable media.

²⁹⁵ See *Supra* at footnote 18 Sally Monaghan.

²⁹⁶ See *Id.*

²⁹⁷ See *Id.*

Mitigating Considerations: A note of caution is needed about the links that connect increased advertising for online gambling with increased problem gambling. First, the connection between increased advertising and aggregate growth of online gambling volume is likely and is supported by forecasts of increased online gambling post legalization.²⁹⁸ However, no research has been done to establish how much of the increase in online gambling is displacement of already existing land-based gambling versus new gamblers or increased activity by existing gamblers. Second, the connection between increased online gambling and increased incidence of problem gambling is also not established. Early research indicates that, at least in mature markets such as the United Kingdom, access to additional gambling opportunities in general and the addition of online gambling opportunities in particular do not appear to increase the incidence of problem gambling.²⁹⁹

Some regulations have been enacted to limit the advertisement of gambling products across various jurisdictions. In the United Kingdom, the introduction of the Gambling Act brought new restrictions on gambling advertising and subjected it to regulation by the Department for Culture, Media and Sport (DCMS), the British Gambling Commission, and the Advertising Standards Agency, as well as its former regulatory bodies, the Broadcast Committee of Advertising Practice (BCAP) and the Committee of Advertising Practice (CAP).³⁰⁰ The various regulations include provisions prohibiting advertising to minors or vulnerable adults, among others.

In addition to these rules, however, the gambling industry has issued a “voluntary” code for socially responsible advertising, which specifically requires that advertisements include the address of the United Kingdom’s problem gambling help website and encourages operators to include responsible gambling messages in their advertisements.³⁰¹ The code also introduces a “watershed” time of 9 p.m., before which any newly permitted forms of gambling cannot be advertised, although the code does allow for the advertising of sports betting around televised

²⁹⁸ As noted in an August 4, 2009 interview with Simon Holliday, Director of H2 Gambling Capital (U.K.). Also, in a note to investors, the investment bank Goldman Sachs predicted a legalized online gambling market in the U.S. worth \$12 billion (more than double the estimated size of the current market). See Jon Parker, “US to legalize online gambling; worth \$12bn, Goldman Sachs predicts,” *eGaming Review*, June 29, 2009, <http://www.egrmagazine.com/news/industry/168682/us-to-legalise-online-gambling-worth-and3612bn-goldman-sachs-predicts.shtml> (last accessed on August 26, 2009). Also, in an analysis provided to a payment processing firm, PricewaterhouseCoopers estimated the federal revenue effect of legalized online gambling to range from \$13.0 billion (with a higher number of states opting out of the legislation) to \$25.9 billion (with a lower number of states opting out) for the period 2010–2019. See PricewaterhouseCoopers, *Estimate of Federal Revenue Effect of Proposal to Regulate and Tax Online Gambling – Executive Summary*, prepared for UC Group, April 24, 2009, <http://www.safeandsecureig.org/media/pwc09.pdf> (last accessed on August 28, 2009).

²⁹⁹ See *Supra* at footnote 292.

³⁰⁰ Simon Fielder and Dominic Hodgkinson, *United Kingdom’s Gambling Industry Adopts Voluntary Code on Advertising Standards*, Pillsbury Winthrop Shaw Pittman LLP, September 2007, <http://www.pillsburylaw.com/siteFiles/Publications/AD40F0C315922BF5A969E8BF6379B2E4.pdf> (last accessed on August 7, 2009).

³⁰¹ See *Id.*

sporting events.³⁰² In Australia, advertising restrictions are determined by the states/territories; most prohibit advertising to minors and the use of misleading statements, while some have no specific regulations.³⁰³ The National Gaming Board of South Africa has set forth guidelines regarding advertising, prohibiting, among others, advertising to minors and advertising that may encourage excessive gambling.³⁰⁴ The U.S. could impose whatever targeted restrictions on advertising deemed necessary or appropriate.

2. Potential Benefits of Legalization

The following sections describe two mechanisms through which regulation could reduce problem gambling. Regulators could implement (1) public policy measures designed to educate the public on the dangers of problem gambling and (2) efforts to provide resources to those affected by problem gambling.³⁰⁵

a. Access to Funding to Increase Awareness of Problem Gambling

If the United States decides to legalize and tax online gambling, significant revenues may accrue from the imposition of taxes and license fees.³⁰⁶ Australia, Costa Rica, Great Britain, Aruba, and Antigua are some of the many countries that have recognized tax benefits from legalizing online gambling.³⁰⁷

The United States could use tax and license revenues to substantially boost publicly funded prevention, counseling, and treatment programs as well as research on gambling addiction.³⁰⁸ Currently, statutes in some states require that information regarding problem gambling be provided to persons participating in any form of legalized gambling. At least three states require that telephone helplines be maintained for problem gamblers.

³⁰² See *Id.*

³⁰³ See Advertising Federation of Australia, *Gambling*, <http://www.afa.org.au/public/content/ViewCategory.aspx?id=509> (last accessed on August 7, 2009).

³⁰⁴ Mpande Advisors, *Report on the Regulation of Interactive Gambling*, prepared for the National Gambling Board of South Africa, October 2005, at p. 50 and 67.

³⁰⁵ See *Supra* at footnote 152. Also see *Supra* at footnote 59 at ¶11–12.

³⁰⁶ Researchers have estimated that at a flat tax rate of 6.25%, online gambling could generate more than \$750 million annually. See *Supra* at footnote 68 Christopher Grohman at p. 68.

³⁰⁷ See *Id.*

³⁰⁸ See *Supra* at footnote 257 Michael Belletire at p. 12–13. Also see General Accounting Office, *Internet Gambling: An overview of the Issues*, GAO-03-89, December 2002; cited by Gerd Alexander, “The U.S. on Tilt: Why the Unlawful Internet Gambling Enforcement Act is a Bad Bet,” *Duke Law & Technology Review*, 5 (2008), at ¶9.

Advocates for problem gamblers have been very vocal about the under-funding in existing budgets for prevention, counseling, and treatment services and observe that most health insurers currently do not cover these services.³⁰⁹ Only 25 states provide any funding for problem gambling programs.³¹⁰ Availability of tax dollars from online gambling revenues and licensing fees could be used to substantially bolster problem-gambling awareness and treatment programs, and to provide educational supports for parents and higher-educational institutions dealing with underage gambling.

b. *Wider Implementation of Responsible Gambling Features*

Legalization of online gambling could lead to the introduction and wider implementation of regulations that give online gamblers tools for controlling their own gambling behaviors.³¹¹

Online gamblers today have access to a variety of online gambling options. However, research indicates the general lack of responsible gambling practices and safeguards offered by these online gambling websites. A 2004 exploratory study of 30 U.K.-based Internet gambling sites found that very few sites engaged in socially responsible practices.³¹² Of the 30 sites, 26 had no reference to a problem gambling help resource; further, 20 sites showed no evidence of social responsibility and 29 sites did not seem to give an option to self-exclude from the site.

Various types of responsible gambling practices have been advocated, including links to problem gambling helplines and websites, self-exclusion programs, and self-imposed time and money limits.³¹³ Some common elements of regulatory structures across leading online gambling jurisdictions include (1) requiring operators to provide players with mechanisms to set their own

³⁰⁹ Franklin discusses lack of federal funding for treatment or awareness of problem gambling, lack of insurance parity for problem gamblers, and limited or lack of funding from most states in the United States. Joanna Franklin, *Problem Gambling in the U.S – From the Beginning into 2001*. Presentation available at Responsible Gambling Council, http://www.responsiblegambling.org/articles/Problem_and_Pathological_Gambling_A_view_from_the_States.pdf (last accessed on September 10, 2009). Also Winslow discusses the lack of state funding for problem gambling services in Colorado and other states in the United States. Kyle Winslow, “A Problem for Gamblers,” *The American Prospect*, March 10, 2008, http://www.prospect.org/cs/articles?article=a_problem_for_gamblers (last accessed on September 10, 2009).

³¹⁰ As noted in a June 5, 2009 interview with Keith Whyte, Executive Director of the National Council on Problem Gambling.

³¹¹ See *Supra* at footnote 152 at p. 15.

³¹² See *Supra* at footnote 24.

³¹³ As noted in a June 10, 2009 interview with Howard Shaffer, Director of the Division on Addictions and Associate Professor of Psychology in the Department of Psychiatry at the Cambridge Health Alliance. Also, as noted in a June 10, 2009 interview with Bo Bernhard, Director of Gambling Research at the UNLV College of Hotel Administration, Nova Scotia recently introduced voluntary loss limits as a self-regulatory device in its land-based gaming operations. Also as noted in an August 5, 2009 interview with Phill Brear, Head of Gambling Regulation at the Gibraltar Regulatory Authority, gambling websites regulated by Gibraltar have responsible gaming features such as “cool-off” periods and self-exclusions mechanisms.

betting limits or limit the deposits they make to their online gambling accounts; (2) requiring site operators to allow gamblers to self-exclude from participating in gambling with the operator; (3) permitting family members to petition to exclude a gambler from a website; (4) banning extension of credit to players; (5) requiring operators to display prominent links to support and counseling services.³¹⁴ In addition to these, the European Gaming and Betting Association lists approximately 50 provisions related to mitigating problem gambling.³¹⁵ U.S. regulators could use this list as a menu from which to identify and evaluate various safeguards. The list includes requiring registration pages to offer self-diagnostic tests designed to help would-be gamblers understand their own attitudes and vulnerabilities, and requiring operators to impose speed-of-play, compulsory time-outs, or player-loss-rate caps.³¹⁶ Aristotle, Inc., mentioned previously, has produced the Integrity Self-Exclusion List (SEL), an international database of people who have chosen to exclude themselves from bricks-and-mortar and online gambling.³¹⁷ If an excluded gambler attempts to open an account, Integrity will not return an approval code from its verification system.³¹⁸ Finally, gambling sites can train staff to identify spending patterns that indicate problem gambling and to contact the gambler directly.³¹⁹

In assessing the general effectiveness of responsible gaming features in the context of online gambling, one 2008 study by researchers at Harvard University demonstrated that responsible gaming safeguards can be effective in the Internet gambling environment. With self-limits, online gamblers reduced their frequency of play—both the number of days on which they placed bets and the number of bets they placed per betting day. The amount they wagered per bet did not change significantly, although the online gamblers did reduce the total amount they wagered.

³²⁰ In a large-scale survey of online gamblers, when asked about the usefulness of including

³¹⁴ See *Supra* at footnote 286 at p. 10–12. Also Grohman notes that the United States could set up a protocol such that banks or other financial institutions must monitor deposits onto sites and report habitual or problem gamblers to proper authorities. In addition, he notes that the government could empower families to monitor problem gamblers by installing monitoring chips in computers. See *Supra* at footnote 68 Christopher Grohman at p. 67. Also see *Supra* at footnote 24. Also see *Supra* at footnote 152 at p. 15. Also see *Australia: Uniform Standards for the Regulation of Interactive Gaming*, The National Working Party on Interactive Gaming, Exposure Draft, April 5, 2001, at p. 22.

³¹⁵ *EGBA Standards Benchmark Study: Overview*, European Gaming & Betting Association, 2008, Table 2, at p. 11–13.

³¹⁶ See *Id.*

³¹⁷ Integrity, *Self-Exclusion List (Online Gaming)*, Aristotle, Inc., http://integrity.aristotle.com/index2.php?option=com_content&do_pdf=1&id=52 (last accessed on August 11, 2009).

³¹⁸ See *Id.*

³¹⁹ As noted in an August 5, 2009 interview with Phill Brear, Head of Gambling Regulation at the Gibraltar Regulatory Authority.

³²⁰ Sarah E. Nelson *et al.*, “Real Limits in the Virtual World: Self-Limiting Behavior of Internet Gamblers,” *Journal of Gambling Studies*, 24 (2008): 463–477, <http://www.divisiononaddictions.org/html/reprints/selflimits.pdf> (last accessed on September 11, 2009), at p. 7.

responsible gambling features, such as self-imposed time limits, self-exclusion, regular financial statements, and regular self-assessments tests, online gamblers indicated that they would find it “quite useful.” The Executive Director of the National Council on Problem Gambling, Keith Whyte, testified before the U.S. Congress as follows:

The graphical and interactive structure of the internet provides a revolutionary opportunity to create informed consumers with access to a variety of information designed to encourage safe choices and discourage unsafe behavior....

The technology also exists, unlike for other forms of gambling, to allow players and operators to set limits on time, wagers, deposits, etc...as well as to exclude themselves.³²¹

D. Concluding Remarks

Legislative restrictions have failed to prevent U.S. gamblers from engaging in online gambling. Rather, those restrictions have led to additional business for Internet gambling operators beyond the regulatory reach of the United States. The current environment lacks responsible gaming features and safeguards offered to gamblers and limits publicly funded resources to educate the populace about problem gambling. We believe that regulators should be able to design sufficient protections to prevent any significant growth in problem gambling that results from legalization. Operators licensed within the United States should be required to offer a best-in-the-world range of services and resources for problem gamblers as well as to prevent underage gambling. Moreover, a proportion of the tax revenues and licensing fees derived from the U.S.-based industry could be used to substantially bolster the level of support for educational programs and services. According to André Wilsenach, head of the Alderney Gambling Control Commission, problem gamblers would receive “clear-cut” benefits from regulated online gambling, since land- and river-based gaming does not provide the tools that are possible in an online environment.³²²

³²¹ Statement of Keith Whyte, in U.S. House of Representatives, Committee on Financial Services, *Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?* 110th Cong., 1st Session, June 8, 2007, at p. 120.

³²² From an August 27, 2009 interview with André Wilsenach.

APPENDIX A

Table 1 provides an overview of the 10 risks, providing for each:

- an indication of protections afforded under the current U.S. regulatory framework;
- an indication of the natural regulatory structure and strategy for control; and
- comments regarding relevant technologies and tactics, and the respective role of other parties.

TABLE 1: Major Categories of Risk Related to Online Gambling

	<u>Category</u>	<u>Existing Protection</u>	<u>Natural Regulatory Structure & Strategy</u>	<u>Relevant Controls & Technologies</u>
1.	Gambling by minors	No effective protection. Offshore sites range from well regulated to completely unregulated.	Industry's short-run incentives: <i>supervisory</i> . Industry's long-run/strategic view: <i>cooperative</i> .	(Strongest form) Positive id matching at player registration against existing databases of known adults. Range of weaker forms of age verification available at player registration. Provision of child-protective software for parents, to keep minors off their parents' accounts.
2.	Consumers defrauded by site operators	No effective protection. Offshore sites range from well regulated to completely unregulated.	<i>Supervisory:</i> Enforcement focus aimed at disreputable operators. Exclusion of bad actors.	Vetting applicants and monitoring existing licensee behavior. Licensee oversight that includes software audits, mystery shopping, and betting pattern monitoring by regulator. Available complaint procedures: players report directly to regulators and have access to U.S. courts.
3.	Players cheated by other players	Detection mostly by other players. Remedies unavailable if sites deny the problem.	<i>Naturally cooperative:</i> Public and industry's interests both served by preserving integrity of games.	Comprehensive data retention by sites. Routine operation of pattern recognition systems for anomaly detection. Complaint procedures available for players to report anomalies to operators and to regulators. Regulatory oversight of complaint investigation and disposition.
4.	Involvement of organized crime	No effective protection with respect to offshore activities.	<i>Supervisory:</i> Enforcement focus aimed at disreputable operators. Exclusion of bad actors.	Vetting applicants and monitoring existing licensees/operators for · criminal backgrounds, · criminal associations, and · hidden ownership interests.
5.	Money laundering by site operators	Offshore operations subject to international cooperative enforcement efforts.	<i>Supervisory:</i> Enforcement focus aimed at disreputable operators. Exclusion of bad actors.	Vetting applicants and monitoring existing licensees/operators for · criminal backgrounds, · criminal associations, and · hidden ownership interests.
6.	Money laundering by players	No effective protection.	Short-run incentives: <i>supervisory</i> . Long-run/strategic view: <i>cooperative</i> .	Anti-money-laundering laws apply. Comprehensive data retention by sites. Details of every transaction recorded (not possible in casinos). Pattern recognition · by operators as part of a compliance operation, and · by regulators as part of oversight audit operation.

TABLE 1 (continued): Major Categories of Risk Related to Online Gambling

	Category	Existing Protection	Natural Regulatory Structure & Strategy	Relevant Controls & Technologies
7.	Violation of jurisdictional restrictions or prohibitions	<p>No effective protection.</p> <p>States have no remedy with respect to offshore sites.</p>	<p>Short-run incentives: <i>supervisory</i>.</p> <p>Long-run/strategic view: <i>cooperative</i>.</p>	<p>Right of government to prohibit or restrict operators within state, and services offered to residents by operators outside of state.</p> <p>Federal regulation of licensees that obliges them to respect list of state exclusions/restrictions.</p> <p>Residence validation at player registration.</p> <p>Geolocation monitoring for each player session (e.g., by ISP analysis).</p> <p>Regulatory audits of operators' software controls.</p> <p>Mystery shopping/testing by states exercising rights to restrict.</p> <p>Federal and state remedy against licensed operators through federal or state law.</p>
8.	Breaches of data confidentiality	<p>No effective protection.</p> <p>Offshore operators outside U.S. jurisdiction.</p>	<p>Short-run incentives: <i>supervisory</i>.</p> <p>Long-run/strategic view: <i>cooperative</i>.</p>	<p>Licensees subject to all U.S.-based requirements regarding data confidentiality.</p> <p>Licensees subject to criminal sanctions and civil liability for breaches/abuses.</p> <p>Data-protection controls subject to audit.</p>
9.	Communications and computer security failures	<p>No effective protection.</p> <p>Offshore operators outside U.S. jurisdiction.</p>	<p>Short-run incentives: <i>supervisory</i>.</p> <p>Long-run/strategic view: <i>cooperative</i>.</p>	<p>Principal responsibility for state-of-the-art security should rest with site operators.</p> <p>Civil liability for site operators with respect to any harm to consumers.</p> <p>Regulator's role in auditing site security software/systems.</p>
10.	Problem gambling behaviors	<p>No effective protection.</p> <p>Offshore sites range from well regulated to completely unregulated.</p>	<p>Short-run incentives: <i>supervisory</i>.</p> <p>Long-run/strategic view: <i>cooperative</i>.</p>	<p>Site-imposed limitations & controls.</p> <p>Self-imposed exclusion options.</p> <p>Self-imposed limiting options.</p> <p>Taxes and license-fee revenue distribution can extend & enhance counseling & support services.</p>

Bibliography

AARP Bulletin. "State Lotteries." AARP, April 2009.

http://bulletin.aarp.org/publish/etc/medialib/aarp_media_library/bulletin/print_issues/april_2009_print.Par.27512.File.dat/April09.pdf (last accessed on July 23, 2009).

Advertising Federation of Australia. *Gambling*.

<http://www.afa.org.au/public/content/ViewCategory.aspx?id=509> (last accessed on August 7, 2009).

Albanese, Jay. "Casino Gambling and Organized Crime: More Than Reshuffling the Deck." In *Contemporary Issues in Organized Crime*, edited by Jay Albanese, 1–15. Monsey, New York: Criminal Justice Press (1995).

Alderney Gambling Control Commission. *The Alderney eGambling Regulations*, 2006.

<http://www.gamblingcontrol.org/userfiles/file/97.pdf> (last accessed on August 19, 2009).

Alexander, Gerd. "The U.S. on Tilt: Why the Unlawful Internet Gambling Enforcement Act is a Bad Bet." *Duke Law & Technology Review*, 5 (2008).

American Gaming Association. *Internet Gambling*. AGA Fact Sheet.

http://www.americangaming.org/Industry/factsheets/issues_detail.cfv?id=17 (last accessed on August 27, 2009).

American Gaming Association. *Money Laundering*. AGA Fact Sheet.

http://www.americangaming.org/Industry/factsheets/issues_detail.cfv?id=3 (last accessed on July 28, 2009).

American Gaming Association. *State of the States: The AGA Survey of Casino Entertainment*, 2006.

http://www.americangaming.org/assets/files/2006_Survey_for_Web.pdf (last accessed on July 23, 2009).

American Gaming Association. *States with Gaming*. AGA Fact Sheet.

http://www.americangaming.org/Industry/factsheets/general_info_detail.cfv?id=15 (last accessed on July 21, 2009).

American Gaming Association. *Suspicious Activity Reporting Policy*.

[http://www.americangaming.org/assets/files/SARC_Policy_\(6\).pdf](http://www.americangaming.org/assets/files/SARC_Policy_(6).pdf) (last accessed on July 28, 2009).

An Exploratory Investigation in the Attitudes and Behaviours of Internet Casino and Poker Players. Report Commissioned by eCOGRA. Nottingham Trent University, 2007.

Anderson, Ross. *Security Engineering, A Guide to Building Dependable Distributed Systems* 2nd Edition. Wiley, 2008.

Annenberg Public Policy Center. *Internet Gambling Stays Low Among Youth Ages 14 to 22 But Access to Gambling Sites Continues; Sports Gambling Makes Resurgence*. University of Pennsylvania, November 26, 2008.

<http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=306> (last accessed on July 25, 2009).

Antigua and Barbuda – Directorate of Offshore Gaming. *Interactive Gaming and Interactive Wagering Regulations*.

http://www.antiguagaming.gov.ag/files/Antigua_and_Barbuda_Gaming_Regulations-Final.pdf (last accessed July 23, 2009).

APWG. *Phishing Activity Trends Report Q1/2008*. January–March 2008.

http://www.antiphishing.org/reports/apwg_report_Q1_2008.pdf (last accessed on August 3, 2009).

Audi, Tamara. “U.S. Deals Blow to Online-Poker Players.” *The Wall Street Journal Online*, June 10, 2009.

<http://online.wsj.com/article/SB124459561862800591.html> (last accessed on August 3, 2009).

Bachus, Spencer. “Online Gambling Leads to Crime and Hurts Young, So Why Encourage It? Asks Spencer Bachus.” *US News & World Report*, June 1, 2009.

<http://www.usnews.com/articles/opinion/2009/06/01/online-gambling-leads-to-crime-and-hurts-young-so-why-encourage-it-asks-spencer-bachus.html> (last accessed on July 30, 2009).

Barrett, Larry. “Major League Baseball Struggles to Reach Fans Online.” *Baseline*, March 7, 2005.

http://www.baselinemag.com/index2.php?option=content&do_pdf=1&id=3506 (last accessed on September 4, 2009).

Belletire, Michael, Steve DuCharm, Dennis Neilander, Frank Catania, Chuck Patton, George Turner, Mel Fisher, Jack Thar, Jack Ketterer, Hillary Crain, and Mac Ryder. *Legislating and Regulating Casino Gaming: A View from State Regulators*. Paper commissioned by the Regulation, Enforcement and Internet Subcommittee of the National Gambling Impact Study Commission, 1999.

Bernhard, Bo J., Anthony F. Lucas, and Elena Shampaner. “Internet Gambling in Nevada.” Prepared for the International Gaming Institute, University of Nevada, Las Vegas (April 2007).

http://gaming.nv.gov/documents/pdf/igi_ngcb_internet_gaming_nvfinalrpt.pdf (last accessed on July 23, 2009).

Bernhard, Bo J., Anthony F. Lucas, and Dongsuk Jang. *Responsible Gaming Device Research Report*. International Gaming Institute. University of Nevada, Las Vegas, 2006.

Blaszczynski, Alex, Robert Ladouceur, and Howard J. Shaffer. “A Science-Based Framework for Responsible Gambling: The Reno Model.” *Journal of Gambling Studies*, 20, No. 3 (Fall 2004): 301–317.

Botzum, Keys. *WebSphere Application Server V6 advanced security hardening -- Part 1, Overview and approach to security hardening*. IBM WebSphere Developer Technical Journal, December 2005.
http://www.ibm.com/developerworks/websphere/techjournal/0512_botzum/0512_botzum1.html
(last accessed on September 14, 2009).

British Gambling Commission. *Conditions and Codes of Practice applicable to: Remote Casino Licences, Remote Casino Ancillary Licences*, December 2008.

British Gambling Commission. *Online Mystery Shopping Programme*. July 2009.
<http://www.gamblingcommission.gov.uk/pdf/online%20mystery%20shopping%20programme%20july%202009.pdf> (last accessed on August 2, 2009).

Brunker, Mike. "Poker 'bots' raking online pots?" *MSNBC.com*, September 21, 2004.
<http://www.msnbc.msn.com/id/6002298/print/1/displaymode/1098/> (last accessed on July 25, 2009).

Cabot, Anthony, and John Aristotle Phillips. "Age Verification: UIGEA Compliance and Regulation." *World Online Gambling Law Report*, October 2006.
<http://integrity.aristotle.com/documents/AgeVerificationLawPublication.pdf> (last accessed on August 10, 2009).

California Office of Privacy Protection. *Recommended Practices on Notice of Security Breach Involving Personal Information*. May 2008.
http://www.oispp.ca.gov/consumer_privacy/pdf/secbreach.pdf (last accessed on July 31, 2009).

Clarke, Roger, and Gillian Dempsey. "The Feasibility of Regulating Gambling on the Internet." *Managerial and Decision Economics*, 22 (2001): 125–132.

Commission on Child Online Protection. *Report to Congress*. October 20, 2000.
<http://www.copacommission.org/report/COPAreport.pdf> (last accessed on August 11, 2009).

Corporation for American Banking. *Due Diligence Report – New Account Opening Procedures*. American Bankers Association, July 2007.

Cotte, June, and Kathryn A. LaTour. "Blackjack in the Kitchen: Understanding Online versus Casino Gambling." *Journal of Consumer Research*, 35 (February 2009): 742–758.

Cunningham, John. *Online Treatment for Addictions*. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Cyberspace Policy Review. *Assuring a Trusted and Resilient Information and Communications Infrastructure*. National Security Council, May 2009.
<http://www.whitehouse.gov/asset.aspx?AssetId=1906> (last accessed on August 2, 2009).

Cyveillance. *The Cost of Phishing: Understanding the True Cost Dynamics Behind Phishing Attacks*. White Paper, December 2008.

http://www.cyveillance.com/web/docs/WP_CostofPhishing.pdf (last accessed on August 3, 2009).

Data Protection Act 2002. Treasury of the Isle of Man. Chapter 2.

<http://www.gov.im/lib/docs/infocentre/acts/dpa2002.pdf> (last accessed on August 4, 2009).

Data Protection in the European Union. European Commission, United Kingdom.

http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-ukingdom_en.pdf (last accessed on July 29, 2009).

Department for Culture, Media and Sport. *Gambling Review Report*. Presented to Parliament by the Secretary of State for Culture, Media and Sport by command of Her Majesty, July 2001.

http://www.culture.gov.uk/reference_library/publications/4642.aspx
(last accessed July 23, 2009).

Derevensky, Jeffrey L. “Youth Gambling and the Internet: The Good, the Bad and the Ugly.” McGill University International Centre for Youth Gambling Problems and High-Risk Behaviours. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Derevensky, Jeffrey L., Laurie Dickson, and Rina Gupta. “Adolescent Attitudes toward Gambling.” *Brazilian Journal of Cognitive Psychology*, 8, No. 1 (2008). http://pepsic.bvs-psi.org.br/scielo.php?script=sci_arttext&pid=S1808-56872008000100002&lng=en&nrm= (last accessed on September 1, 2009).

Dhamija, Rachna, J.D. Tygar, and Marti Hearst. “Why Phishing Works.” *Experimental Social Science Laboratory (Xlab)*, Paper XL06-013 (August 14, 2006): 581–590.

<http://repositories.cdlib.org/iber/xlab/XL06-013> (last accessed on August 3, 2009).

Draft Regulatory Control Model for New Forms of Interactive Home Gambling. Developed by a meeting of Gaming Ministers in Australia, May 23, 1997.

Dunstan, Roger. “Gambling in California.” *California Research Bureau*.

<http://www.library.ca.gov/crb/97/03/crb97003.html#toc> (last accessed on July 26, 2009).

European Commission. Background Report on Cross Media Rating and Classification, and Age Verification Solutions. Safer Internet Forum, September 2008.

http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/reportage_verification.pdf (last accessed on August 24, 2009).

European Gaming & Betting Association. *EGBA Standards Benchmark Study*, 2008.

Fabuli, Marvin. *Online Casinos an Easy Bet for Phishers*. Symantec, February 27, 2008.

<http://www.symantec.com/connect/blogs/online-casinos-easy-bet-phishers> (last accessed on August 3, 2009).

Federal Communications Commission. Report in the Matter of Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming. MB Docket No. 09-26, released August 31, 2009.

http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-69A1.pdf
(last accessed on September 1, 2009).

Fielder, Simon, and Dominic Hodgkinson. *United Kingdom's Gambling Industry Adopts Voluntary Code on Advertising Standards*. Pillsbury Winthrop Shaw Pittman LLP, September 2007.

<http://www.pillsburylaw.com/siteFiles/Publications/AD40F0C315922BF5A969E8BF6379B2E4.pdf> (last accessed on August 7, 2009).

Financial Crimes Enforcement Network. *A Survey of Electronic Cash, Electronic Banking, and Internet Gaming*. U.S. Department of the Treasury, 2000.

Financial Crimes Enforcement Network. *The SAR Activity Review – Trends, Tips & Issues*. May 13, 2008.

http://www.fincen.gov/news_room/rp/files/sar_tti_13.pdf (last accessed on August 5, 2009).

Franklin, Joanna. *Problem Gambling in the U.S: From the Beginning – Into 2001*. Trimeridian Inc, 2001.

http://www.responsiblegambling.org/articles/Problem_and_Pathological_Gambling_A_view_from_the_States.pdf (last accessed on July 14, 2009).

Full Tilt Poker. *Privacy*. <http://www.fulltiltpoker.com/privacy-legal.php> (last accessed on July 29, 2009).

Gambling Act, 2005 Chapter 19 (Eng.).

GamCare. *Press Release – Underage Internet Gambling Study*. July 27, 2004.

http://www.gamcare.org.uk/news.php/27/press_release_underage_internet_gambling_study (last accessed on September 11, 2009).

GamesandCasino.com. *Blacklisted Casinos*.

<http://www.gamesandcasino.com/blacklist.htm> (last accessed on July 23, 2009).

Gass, Kevin. *BCLC the New Age of Gaming*. BCLC. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Gaul, Gilbert M. “Players Gamble on Honesty, Security of Internet Betting.” *The Washington Post*, November 30, 2008, p. A12.

General Accounting Office. *Internet Gambling: An Overview of the Issues*. GAO-03-89. Report to Congressional Requesters, December 2002.

Germain, Jack M. "Global Extortion: Online Gambling and Organized Hacking." *Tech News World*, March 23, 2004.
<http://www.technewsworld.com/story/33171.html?wlc=1248627730>
(last accessed on July 26, 2009).

Gibraltar Gambling Act 2005.
<http://www.gra.gi/sites/gambling/downloads/42/gambling%20ord%202005.pdf> (last accessed on August 6, 2009).

Gibraltar Regulatory Authority. *Code of Practice for the Gambling Industry*. Issued by the Gambling Commissioner, December 13, 2008.
http://www.gra.gi/sites/gambling/downloads/215/generic_code_v1.0.2009.pdf (last accessed on August 6, 2009).

Glass, Loris. "Gambling Education: Some Strategies for South Australian Schools." Funded by the Gamblers Rehabilitation Fund, South Australia, November 2002.
<https://www.library.health.sa.gov.au/Portals/0/gambling-education-some-strategies-for-south-australian-schools.pdf> (last accessed on September 2, 2009).

Goldman, Russell. "Online Poker Players Expose Alleged Fraud." *ABC News*, October 19, 2007. <http://abcnews.go.com/print?id=3752500> (last accessed on July 24, 2009).

Gottfried, Jonathan. "The Federal Framework for Internet Gambling." *Richmond Journal of Law & Technology*, X, No. 3.
<http://law.richmond.edu/jolt/v10i3/article26.pdf> (last accessed on August 6, 2009).

Greenberg, Andy. "Cybercops Without Borders." *Forbes.com*, June 1, 2009.
<http://www.forbes.com/2009/06/01/cyberbusts-security-internet-technology-security-cyberbusts.html> (last accessed on July 27, 2009).

Griffiths, Mark D. "Does Gambling Advertising Contribute to Problem Gambling?" *International Journal of Mental Health & Addiction*, 3, No. 2 (2005): 15–25. <http://ijma-journal.com/pdf/v3i2a02.pdf> (last accessed on September 2, 2009).

Griffiths, M.D. "Internet Gambling: Issues, Concerns and Recommendations." *CyberPsychology & Behavior*, 6, No. 6 (2003): 557–568. Cited in Sarah E. Nelson *et al.* "Real Limits in the Virtual World: Self-Limiting Behavior of Internet Gamblers." *Journal of Gambling Studies*, 24 (2008): 463–477.

Grimes, Roger A. "How to Develop an Enterprise Encryption Strategy." *InfoWorld*, September 1, 2006. <http://www.infoworld.com/print/24540> (last accessed on July 31, 2009).

Grohman, Christopher. "Reconsidering Regulation: A Historical View of the Legality of Internet Poker and Discussion of the Internet Gambling Ban of 2006." *Journal of Legal Technology Risk Management*, 1, No. 1 (Fall 2006): 34–74.

Hills, Chad. Internet Gambling: Irresponsible Policy
<http://www.citizenlink.org/FOSI/gambling/A000004244.cfm> (last accessed on July 11, 2009).

Holliday, Simon, David Henwood, Michael Bradbury, and Phil Martin. *Internet Gambling Market Overview: AGA Internet Gaming Task Force*. H2 Gambling Capital, December 2, 2008.

Hornbuckle, William J. Letter and Presentation to U.S. House of Representatives, Subcommittee Hearing on H.R. 21 (Unlawful Internet Gambling Funding Prohibition Act), April 2003.

Hugel, Paul, and Joseph Kelly. "Internet Gambling, Credit Cards and Money Laundering." *Journal of Money Laundering Control*, 6, No. 1 (2002): 57–65.

Identity Theft Daily staff. "Identity Theft News: 2008 Data Breach count is 69% greater than 2007." *Identify Theft Daily*.

<http://www.identitytheftdaily.com/index.php/20080716371/Latest/Identity-Theft-News-2008-Data-Breach-count-is-69-greater-than-2007.html>
(last accessed on July 29, 2009).

Illinois Gaming Board. Minimum Internal Control Standards – Section J-Currency Transaction Reporting and Suspicious Activity Reporting, October 1, 2007.

Integrity. *Case Study: Age Verification for Online Alcohol Sales*. Aristotle, Inc.
http://integrity.aristotle.com/documents/Online_Wine_Sales-WhitePaper2006.pdf (last accessed on August 11, 2009). Integrity. *Integrity: Direct*. Aristotle Inc.

http://integrity.aristotle.com/index2.php?option=com_content&do_pdf=1&id=47 (last accessed on August 11, 2009).

Integrity. Self-Exclusion List (Online Gaming). Aristotle, Inc.

http://integrity.aristotle.com/index2.php?option=com_content&do_pdf=1&id=52 (last accessed on August 11, 2009).

Interactive Gaming Council. "Online Gambling Sites Less Susceptible to Money Laundering Than Real-World Counterparts." *Winner Online*, September 24, 2002.

<http://www.winneronline.com/articles/september2002/fatf.htm> (last accessed on August 5, 2009).

International Game Technology. *Online Gaming in a Regulated Environment*. Presentation to the American Gaming Association.

International Organization for Standardization. *Information Security Management Systems*.

http://www.iso.org/iso/iso_catalogue/management_standards/specific_applications/specific_applications_it-security.htm (last accessed on July 31, 2009).

Internet Gambling Regulation and Tax Enforcement Act of 2009, H.R. 2268, 111th Cong. (2009). http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h2268ih.txt.pdf (last accessed on August 28, 2009).

Internet Gambling Regulation, Consumer Protection, and Enforcement Act, H.R. 2267, 111th Cong. (2009). http://www.house.gov/apps/list/press/financialsvcs_dem/21frank_008_xml.pdf (last accessed on July 23, 2009).

Internet Safety Technical Task Force. *Enhancing Child Safety and Online Technologies*. Final Report to the Multi-State Working Group on Social Networking of State Attorneys. Berkman Center for Internet & Society, Harvard University, December 31, 2008. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf (last accessed on September 11, 2009).

Isle of Man Gambling Supervision Commission. *Online Gambling – Guidance Notes for the Prevention of Money Laundering and Countering of Terrorist Financing*, April 2009 (draft version). <http://www.gov.im/lib/docs/gambling//onlinegamblingguidancenotesamlc.doc> (last accessed on July 23, 2009).

Jonsson, Jakob. *Responsible Gaming and Gambling Problems among 3000 Swedish Internet Poker Players*. Spelinstitutet. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Kahnawake Gaming Commission. *In the Matter of Absolute Poker – Investigation regarding Complaints of Cheating*. January 11, 2008. <http://www.kahnawake.com/gamingcommission/KGC-AP-0111.pdf> (last accessed on July 24, 2009).

Kahnawake Gaming Commission. *Kahnawake Gaming Commission Imposes Sanctions on Ultimate Bet with Regard to Cheating Incidents*. September 29, 2008. <http://www.kahnawake.com/gamingcommission/kgc092908.pdf> (last accessed on July 24, 2009).

Kahnawake Gaming Commission. *Permit Holders*. <http://www.kahnawake.com/gamingcommission/> (last accessed on July 24, 2009).

Kahnawake Gaming Commission. *Regulations Concerning Interactive Gaming*. Last amended on March 29, 2007. <http://www.kahnawake.com/gamingcommission/Kahnawake%20Regulations%20Concerning%20Interactive%20Gaming.pdf> (last accessed on July 24, 2009).

Kaplan, Dan. “Leahy, for Third Time, Submits Federal Data Security Law.” *SC Magazine*, July 24, 2009. <http://www.scmagazineus.com/Leahy-for-third-time-submits-federal-data-security-law/article/140604/> (last accessed on July 29, 2009).

Keizer, Gregg. "Microsoft promises patch for critical Web server bug." *Computerworld*, September 2, 2009.

http://www.computerworld.com/s/article/9137438/Microsoft_promises_patch_for_critical_Web_server_bug (last accessed on September 9, 2009).

King, Kevin F. "Cutting Internet Gambling's Gordian Knot: Geolocation and Federalism on the Internet." *Northwestern University Law Review*, July 14, 2009, available at SSRN: <http://ssrn.com/abstract=1433634> (last accessed on July 20, 2009).

King, Rachel. "Lessons from the Data Breach at Heartland." *Business Week*, July 7, 2009. <http://www.msnbc.msn.com/id/31778540/ns/business-businessweekcom/> (last accessed on July 29, 2009).

Kinnee, Kevin B. *Practical Gambling Investigation Techniques*. New York: Elsevier (1992).

LaBrie, Richard A., Debi LaPlante, Sarah E. Nelson, Anja Schumann, and Howard J. Shaffer. "Assessing the Playing Field: A Prospective Longitudinal Study of Internet Sports Gambling Behavior." *Journal of Gambling Studies*, 23, No. 3 (2007): 347–362.

LaBrie, Richard A., Sara A. Kaplan, Debi LaPlante, Sarah E. Nelson, and Howard J. Shaffer. "Inside the Virtual Casino: A Prospective Longitudinal Study of Actual Internet Casino Gambling." *The European Journal of Public Health*, 18, No. 4 (2008): 410–416.

LaBrie, Richard. What Do Gaming Regulators Regulate? A Public Health Perspective on Disordered Gambling & Regulation. Presentation before the North American Gaming Regulators Association, 2006.

Ladouceur, Robert, Francine Ferland, Christiane Poulin, Frank Vitaro, and Jamie Wiebe. "Concordance between the SOGS-RA and the DSM-IV Criteria for Pathological Gambling among Youth." *Psychology of Addictive Behaviors*, 19, No. 3 (2005): 271–276.

Landes, Ryan. Layovers and Cargo Ships: The Prohibition of Internet Gambling and a Proposed System of Regulation, *New York University Law Review*, 82, No. 3 (2007): 913–943.

LaPlante, D. A., and H. J. Shaffer. "Understanding the Influence of Gambling Opportunities: Expanding Exposure Models to Include Adaptation." *American Journal of Orthopsychiatry*, 77, No. 4 (2007): 616–623.

LaPlante, Debi A., John H. Kleschinsky, Richard A. LaBrie, Sarah E. Nelson, and Howard J. Shaffer. "Sitting at the Virtual Poker Table: A Prospective Epidemiological Study of Actual Internet Poker Gambling Behavior." *Computers in Human Behavior*, 25, No. 3 (2009): 711–717.

MarkMonitor. Rock Phishing: The Threat and Recommended Countermeasures. White Paper, August 2007.

<http://www.markmonitor.com/download/wp/wp-rockphish.pdf> (last accessed on August 3, 2009).

McBride, Jessica. "Internet Gambling among Youth: A Preliminary Examination." *International Centre for Youth Gambling Problems & High-Risk Behaviors Newsletter*, 6, No. 1 (2006).

McCormick, Amanda. *Review of Online Gambling Literature*. British Columbia Center for Social Responsibility, 2007.

http://www.bccsr.ca/files/Literature%20Review_%20Online%20Gambling.pdf (last accessed on August 5, 2009).

McGraw, Gary, and Ming Chow. "Securing Online Games – Safeguarding the Future of Software Security." *IEEE Security & Privacy*, 7, No. 3 (May/June 2009).

McMullan, John, and Aunshul Rege. *Cheating and Cybercrimes @ Gambling Sites.com*. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

McMullan, John, and David Perrier. "The Security of Gambling and Gambling with Security: Hacking, Law Enforcement and Public Policy." *International Gambling Studies*, 7, No. 1 (2007): 43–58.

McGowan, Richard. *The Gambling Debate*. Westport, CT: Greenwood Press (2008).

MHA Consulting. "The Threat of Money Laundering and Terrorist Financing through the Online Gambling Industry." Report prepared for the Remote Gambling Association, June 2009.

Monaghan, Sally. *Internet and Wireless Gambling – A Current Profile*. Prepared for the Australasian Gaming Council, May, 2008.

http://www.austgamingcouncil.org.au/images/pdf/Discussion_Papers/agc_dis_internet.pdf (last accessed on July 11, 2009).

Monaghan, Sally, Jeffrey Derevensky, and Alyssa Sklar. "Impact of Gambling Advertisements and Marketing on Children and Adolescents: Policy Recommendations to Minimize Harm." *Journal of Gambling Issues*, 22 (December 2008): 252–274.

Mpande Advisors. *Report on the Regulation of Interactive Gambling*. Prepared for the National Gambling Board of South Africa, October 2005.

National Centre for Academic Research into Gaming. *Internet Gaming and South Africa: Implications, Costs & Opportunities*. Interim Report for the National Gambling Board, Cape Town, South Africa, August 1999.

National Conference of State Legislatures. *State Security Breach Notification Laws*. As of July 27, 2009. <http://www.ncsl.org/Default.aspx?TabId=13489> (last accessed on July 31, 2009).

National Council on Problem Gambling. *FAQs – Problem Gamblers*. <http://www.ncpgambling.org/i4a/pages/Index.cfm?pageID=3315> (last accessed on July 11, 2009).

National Gambling Impact Study Commission. National Gambling Impact Study Commission – Final Report. 1999. <http://govinfo.library.unt.edu/ngisc/reports/fullrpt.html> (last accessed on July 23, 2009).

National Research Council. *Pathological Gambling: A Critical Review*. Washington, DC: National Academy Press, 2005.

National Working Party on Interactive Gaming. *Australia: Uniform Standards for the Regulation of Interactive Gaming (The AUS Model)*. Exposure Draft, April 2001.

Nelson, Sarah E. *Actual Internet Gambling – Findings from a Longitudinal Study of Internet Gambling Behavior*. Division on Addictions, Cambridge Health Alliance, Harvard Medical School. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Nelson, Sarah E., Debi A. LaPlante, Allyson J. Peller, Anja Schumann, Richard A. LaBrie, and Howard J. Shaffer. “Real Limits in the Virtual World: Self-Limiting Behavior of Internet Gamblers.” *Journal of Gambling Studies*, 24 (2008): 463–477.

<http://www.divisiononaddictions.org/html/reprints/selflimits.pdf> (last accessed on September 11, 2009).

Nevada Revised Statutes.

New Jersey Permanent Statutes.

Net Nanny. *Protecting Your Family on the Internet*. White paper. http://www.netnanny.com/products/netnanny/protecting_your_family (last accessed on September 10, 2009).

NFC Global. *Internet Gaming & Money Laundering: Measuring the Scope, Assessing the Risks*. Prepared for the Interactive Gaming Council, Vancouver, British Columbia, Canada, August 2005.

Nova Scotia Gaming Corporation. *World-Leading Software Launched to Protect Nova Scotia Youth*. Media Release, May 29, 2009. http://www.nsgc.ca/pdf/press/Microsoft%20Word%20-%20BetStopper%20Media%20Release%20FINAL_May%2028%20w%20photo.pdf (last accessed July 25, 2009).

Office of Congressman Barney Frank. *Frank Unveils Internet Gambling Legislation*. House Committee on Financial Services, May 6, 2009.

Office of Senator Patrick Leahy. *Leahy Introduces Cybersecurity Legislation*. July 22, 2009. <http://leahy.senate.gov/press/200907/072209b.html> (last accessed on July 29, 2009).

Online Casino Advisor. *Harvard Addiction Expert Says Online Gambling No Problem.*” Responsible Gambling Council, April 16, 2009.
http://www.responsiblegambling.org/staffsearch/latest_news_articles_details.cfm?intID=12079
(last accessed on August 5, 2009).

Online Casino City. *Online Gambling Operations in Queens Busted.* November 16, 2006.
<http://online.casinocity.com/article/online-gambling-operation-in-queens-busted-68919>
(last accessed on September 11, 2009).

Online Casino City. *Online Gaming Jurisdictions.* <http://online.casinocity.com/jurisdictions> (last accessed on September 14, 2009).

Online Gaming Monitoring. Pokerpages.com. <http://www.pokerpages.com/> (last accessed on April 17, 2009).

Owens, Martin, and Guy C. Clark. “Internet Gambling Deserves a New Chance.” The Debate Room, *Businessweek*, 2007.
http://www.businessweek.com/debateroom/archives/2007/09/internet_gambli.html (last accessed on July 23, 2009).

Palmer, Maija. “EU plans tougher cybercrime laws.” *FT.com*, June 14, 2009.
<http://www.ft.com/cms/s/0/10a407b6-5913-11de-80b3-00144feabdc0.html> (last accessed on August 2, 2009).

Parke, Jonathan, Adrian Parke, Richard Wood, and Jane Rigbye. *An Exploratory Investigation into the Attitudes and Behaviors of Online Casino and Poker Players.* University of Salford. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Parker, Jon. “US to legalise online gambling; worth \$12bn, Goldman Sachs predicts.” *eGaming Review*, June 29, 2009.
<http://www.egrmagazine.com/print/news/industry/168682/us-to-legalise-online-gambling-worth-and3612bn-goldman-sachs-predicts.shtml> (last accessed on August 26, 2009).

PCI Security Standards Council. *About the PCI Data Security Standard (PCI DSS).*
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (last accessed July 31, 2009).

Pearson, Tricia. “Can I see some ID?” Why age verification is a hot topic for online retailers. Shoosmiths, June 24, 2009.
<http://www.shoosmiths.co.uk/news/2372.asp> (last accessed on August 11, 2009).

Petry, N. M., Frederick S. Stinson, and Bridget F. Grant. “Comorbidity of DSM-IV Pathological Gambling and Other Psychiatric Disorders: Results from the National Epidemiologic Survey on Alcohol and Related Conditions.” *Journal of Clinical Psychiatry*, 66, No. 5 (2005): 564–574.

PGP Corporation. *2008 Annual Study: Cost of a Data Breach*. Study conducted by the Ponemon Institute, LLC, February 2009.

http://www.encryptionreports.com/download/Ponemon_COB_2008_US_090201.pdf
(last accessed on July 31, 2009).

Poker News Daily. “Minnesota Rescinds Internet Gambling Notices to ISPs after iMEGA Settlement.” June 8, 2009.

<http://www.pokernewsdaily.com/minnesota-rescinds-internet-gambling-notices-to-isps-after-imega-settlement-2749/> (last accessed on August 10, 2009).

Poker Players Alliance. PPA Statement on Southern District of NY Action Against Online Poker Players. June 9, 2009.

<http://www.scribd.com/doc/16266358/NY-PPA-Statement-on-Southern-District-of-NY-Action-Against-Online-Poker-Players-PPA-060909>
(last accessed on July 22, 2009).

Poker Stars. Data Privacy for our Poker Software

<http://www.pokerstars.com/poker/room/features/security/> (last accessed on July 24, 2009).

Poker Stars. *Interactive Gaming Council*. <http://www.pokerstars.com/igc/> (last accessed on July 24, 2009).

Poker Stars. *Isle of Man Gambling Supervision Commission*. <http://www.pokerstars.com/iom/>
(last accessed on July 24, 2009).

Poker Stars. Online Poker Privacy Policy.

<http://www.pokerstars.com/poker/room/privacy/#a4> (last accessed on July 29, 2009).

PricewaterhouseCoopers. *Estimate of Federal Revenue Effect of Proposal to Regulate and Tax Online Gambling – Executive Summary*. Prepared for UC Group, April 24, 2009.

<http://www.safeandsecureig.org/media/pwc09.pdf> (last accessed on August 28, 2009).

Public Citizen. Mutual Recognition Agreements (MRAs).

<http://www.citizen.org/trade/harmonization/MRA/> (last accessed on August 10, 2009).

Quova. “The Factors of Geolocation.” *iGaming Business*.

<http://gw.vtrenz.net/index.cfm?method=cMicrositeSecurity.displayLogin&dkey=XOV3IU9JU5>
(last accessed on July 21, 2009).

Quova. *GeoPoint by Quova*. White Paper, July 2006.

https://www1.vtrenz.net/emarkownerfiles/ownerassets/818/GeoPointbyQuova_WHITEPAPER.pdf
(last accessed on July 21, 2009).

Quova. *Quova Helps the Alaska Permanent Fund Dividend Division Run Like a Well-Oiled Machine*. Quova Case Study, 2008.

https://www.vtrenz.net/imaeds/ownerassets/818/08277_Alaska_casestudy_REV2.pdf
(last accessed on August 18, 2009).

Quova. The Science of Geolocation.

<http://www.quova.com/Technology/thescienceofgeolocation.aspx> (last accessed on September 4, 2009).

Reasonable Prudence in Regulation Act, H.R. 2266, 111th Cong. (2009).

http://www.house.gov/apps/list/press/financialsvcs_dem/gambling2.pdf (last accessed on July 23, 2009).

Responsible Gaming Quarterly, “Real-Time Betting Analysis of Internet Casino Gambling,” 6, No. 2 (Fall 2008).

http://www.americangaming.org/assets/files/RGQ_Fall_08.pdf (last accessed on August 10, 2009).

Reznikov, Boris. “Can I See Some ID? Age Verification Requirements for the Online Liquor Store.” *Shidler Journal for Law, Commerce & Technology*, 4, No. 5 (2007).

<http://www.lctjournal.washington.edu/Vol4/a05Reznikov.html> (last accessed on July 25, 2009).

Rini, Bill. *The Definitive Guide to Online Poker Cheating*. April 16, 2008.

<http://www.billrini.com/2008/04/16/the-definitive-guide-to-online-poker-cheating/> (last accessed on July 25, 2009).

Robertson, Jordan. “Tech 101: How a Denial-of-Service Attack Works.” *Associated Press*, July 8, 2009.

<http://www.usnews.com/articles/science/2009/07/08/tech-101-how-a-denial-of-service-attack-works.html?PageNr=1> (last accessed on July 28, 2009).

RSe Consulting. A Literature Review and Survey of Statistical Sources on Remote Gambling. October 2006.

http://www.culture.gov.uk/images/publications/RemoteGambling_RSeReport.pdf (last accessed on July 25, 2009).

Rush, Brian, Scott Veldhuizen and Edward Adlaf. “Mapping the prevalence of problem gambling and its association with treatment accessibility and proximity to gambling venues.” *Journal of Gambling Issues*, 20 (June 2007): 193–214.

Satre, Philip G. *Youth Gambling: The Casino Industry’s Response*. Adapted from address to Harvard Think Tank on Youth Gambling Issues, April 6, 1995.

Scharf, Michael P., and Melanie K. Corrin. “On Dangerous Ground: Passive Personality Jurisdiction and the Prohibition of Internet Gambling.” *New England Journal of International and Comparative Law*, 8, No. 1 (2002).

Schopper, Mark D. “Internet Gambling, Electronic Cash & Money Laundering: The Unintended Consequences of a Monetary Control Scheme.” *Chapman Law Review*, 5, No. 1 (2002): 303-330.

Schorow, Stephanie. "Going for Broke – Professor Says Vegas Gambling Machines Designed to Get People to 'Play to Extinction.'" *MIT TechTalk*, 53, No. 26 (May 20, 2009): 8.

Security and Accountability for Every Port Act. Public Law No. 109-347.

Shaffer, H. J., and M. N. Hall. "Updating and Refining Prevalence Estimates of Disordered Gambling Behaviour in the United States and Canada." *Canadian Journal of Public Health*, 92, No. 3 (2001): 168–172.

Shaffer, H. J., Matthew N. Hall, and Joni Vander Bilt. "Estimating the Prevalence of Disordered Gambling Behavior in the United States and Canada: A Meta-Analysis." Boston: Presidents and Fellows of Harvard College, 1997.

Shaffer, H. J., Matthew N. Hall, and Joni Vander Bilt. "Estimating the Prevalence of Disordered Gambling Behavior in the United States and Canada: A Research Synthesis." *American Journal of Public Health*, 89, No. 9 (1999): 1369–1376.

Skolnick, Jerome H. "The Social Transformation of Vice." *Law and Contemporary Problems*, 51, No. 1 (Winter 1988): 9–29.

Smeaton, Michael and Mark Griffiths. "Internet Gambling and Social Responsibility: An Exploratory Study." *CyberPsychology & Behavior*, 7, No. 1 (2004): 49–57.

Srinivasan, G. "EU slams US on its remote gambling, betting laws." *Business Line*, June 14, 2009.

<http://www.thehindubusinessline.com/2009/06/14/stories/2009061450870400.htm> (last accessed on June 30, 2009).

Stewart, David O. *An Analysis of Internet Gambling and its Policy Implications*. Prepared for AGA 10th Anniversary White Paper Series on Internet Gambling, 2006.

Stop predatory gambling.org. *The 'Perfect Storm' of Harm*.
<http://ncalg.org/internet%20gambling.htm> (last accessed on July 11, 2009).

Sullum, Jacob. "Some Bets Are Off: The Strangely Selective and Self-defeating Crackdown on Internet Gambling." *Reason Online*, June 2008.

<http://www.reason.com/news/show/126022.html> (last accessed on July 23, 2009).

Svantesson, D. J. B. "How Does the Accuracy of Geo-Location Technologies Affect the Law?" *Masaryk University Journal of Law and Technology*, 2, No. 1 (Summer 2008): 11–21.

Sychold, Martin. *Public and Private Sector Internet Gambling Operations: Some Useful Information from Europe*. Swiss Institute of Comparative Law. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Testimony of John G. Malcolm Before the Committee on Banking, Housing, and Urban Affairs. March 18, 2003.

<http://www.usdoj.gov/criminal/cybercrime/malcolmTestimony318.htm> (last accessed on July 29, 2009).

Todd, Aaron. *NETeller Exit Impacts U.S. Internet Gambling Market*. Online Casino City, January 18, 2007.

<http://online.casinocity.com/news/news.cfm?ArticleId=70015> (last accessed on July 13, 2009). Cited by Gerd Alexander, "The U.S. on Tilt: Why the Unlawful Internet Gambling Enforcement Act is a Bad Bet," *Duke Law & Technology Review*, No. 5 (2008).

U.K. Department for Culture, Media and Sport. "Gambling Act 2005 – Advertising Media Fact Pack." August 2007.

<http://www.culture.gov.uk/images/publications/Mediapackadvertisingaug07.pdf> (last accessed on July 31, 2009).

USApayers.com. USA Poker Deposit Methods.

<http://www.usaplayers.com/poker/deposit-methods/index.html> (last accessed on August 8, 2009)

USApayers.com *Online Poker Deposits and the UIGEA*, <http://www.usaplayers.com/deposit-methods/articles/poker/online-poker-deposits-and-the-uigea.html> (last accessed on August 8, 2009).

U.S. House of Representatives. Committee on Financial Services. *Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?* 110th Cong., 1st Session, June 8, 2007.

U.S. House of Representatives. Committee on the Judiciary. *Establishing Consistent Enforcement Policies in the Context of Online Wagers*. 110th Cong., 1st Session, November 14, 2007.

UltimateBet.com. *Status Update on NioNio Investigation*. July 8, 2008.

<http://www.ultimatebet.com/poker-news/2008/july/Investigation-Status-Update> (last accessed on July 24, 2009).

UltimateBet.com. *UltimateBet Issues Statement Regarding Unfair Play*. May 29, 2008.

<http://www.ultimatebet.com/poker-news/2008/may/NioNio-Findings> (last accessed on July 24, 2009).

United States Department of Justice. *Chapter 1 – Computer Fraud and Abuse Act*. Computer Crime & Intellectual Property Section.

<http://www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.pdf> (last accessed on July 29, 2009).

Verrinder, Matthew. "NETeller Ex-Directors on Money Laundering Charges." *Reuters*, January 16, 2007.

<http://www.reuters.com/article/internetNews/idUSN1622302920070116> (last accessed on September 11, 2009).

Wardle, Heather, Kerry Sprotson, Jim Orford, Bob Erens, Mark Griffiths, Rebecca Constantine, and Sarah Pigott. *British Gambling Prevalence Survey 2007*. National Centre for Social Research. Prepared for the Gambling Commission, September 2007.

<http://www.gamblingcommission.gov.uk/pdf/British%20Gambling%20Prevalence%20Survey%2007%20-%20Sept%202007.pdf> (last accessed on August 7, 2009).

Watson, Stevie, Pearson Liddell Jr., Robert S. Moore, and William D. Eshee Jr. "The Legalization of Internet Gambling: A Consumer Protection Perspective." *Journal of Public Policy & Marketing*, 23, No. 2 (2004): 209–213.

Wellford, Charles. "When It's No Longer a Game: Pathological Gambling in the United States." *National Institute of Justice Journal*, April 2001: 14–18.

Wiebe, Jamie. *Player Protection with Internet Gambling*." Factz Research, Inc., Responsible Gambling Council. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Wiebe, Jamie, and Michael Lipton. *An Overview of Internet Gambling Regulations*. Submitted to the Ontario Problem Gambling Research Centre, August 2008.

Wiebe, Jamie and Rachel A. Volberg. *Problem Gambling Prevalence Research: A Critical Overview*. A report to the Canadian Gaming Association. December, 2007.

http://canadiangamingassociation.com/media_uploads/pdf/78.pdf (last accessed on July 11, 2009).

Williams, Robert, and Robert Wood. *Internet Gambling: Setting the Stage*. University of Lethbridge. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Winslow, Kyle. "A Problem for Gamblers." *The American Prospect*, March 10, 2008. http://www.prospect.org/cs/articles?article=a_problem_for_gamblers (last accessed on July 13, 2009).

Wire Act of 1961. 18 U.S.C. §1084(a).

Wood, Richard T. A. *Online Support for People with Gambling Issues*. GamRes Limited. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

Wood, Richard T. A., and Mark D. Griffiths. "Why Swedish People Play Online Poker and Factors That Can Increase or Decrease Trust in Poker Web Sites: A Qualitative Investigation." *Journal of Gambling Issues*, 21 (July 2008): 80–97.

Wood, Robert, and Robert Williams. *Internet Gambling in Comparative Perspective: Patterns, Problems, and Interventions*. University of Lethbridge. Presentation to the Alberta Gambling Research Institute Annual Conference, March 2009.

List of Individuals Interviewed

<u>Name</u>	<u>Date of Interview</u>
Parry Aftab Executive Director Wired Safety	05/27/2009
Bo Bernhard Director of Gambling Research UNLV College of Hotel Administration	06/10/2009
Michael Bolcerek Senior Vice-President of Business Development Aristotle	08/10/2009
Phill Brear Head of Gambling Regulation Gibraltar Regulatory Authority	08/05/2009
Peter Collins Professor of Public Policy Studies, Director of the Center for the Study of Gambling University of Salford (U.K.)	06/10/2009
Philip J. Cook Senior Associate Dean for Faculty and Research, ITT/ Terry Sanford Professor of Public Policy, Professor of Economics and Sociology Duke University	06/10/2009
Kelli Emerick Executive Director Secure ID Coalition	08/06/2009
Andrew Fritchie General Counsel PartyGaming PLC	08/21/2009
Glenn Gibson Manager, Technical and Systems Audit Tasmanian Gaming Commission (Australia)	08/05/2009

Damien Jarvis Assistant Director Liquor and Gaming Branch Tasmania Department of Treasury and Finance (Australia)	08/05/2009
Matthew Hill Director of Strategy, Research and Analysis British Gambling Commission (U.K.)	06/12/2009
Simon Holliday Director H2 Gambling Capital (U.K.)	08/04/2009
Joseph Kelly Professor SUNY Buffalo Business Law	06/01/2009
Paul Mathews Former Senior Vice President IGT Wagerworks	08/03/2009
Sam McQuade Graduate Program Coordinator College of Applied Science and Technology, Rochester Institute of Technology	06/03/2009
Katharina Riedl bwin (Austria)	08/13/2009
Paul Morris Policy Development Manager British Gambling Commission (U.K.)	06/12/2009
Chris Pinion National Account Manager LexisNexis Risk and Information Analytics	08/10/2009
Sue Schneider Founder Interactive Gaming News	08/17/2009
John Sealy Manager, Information Systems and Technology Services Licensing, Regulation and Alcohol Strategy Northern Territory Department of Justice (Australia)	08/31/2009

Howard Shaffer Director of Division on Addictions Associate Professor of Psychology, Department of Psychiatry The Cambridge Health Alliance, Harvard Medical School	06/10/2009
Charles Wellford Professor of Criminology and Criminal Justice University of Maryland, College Park	06/17/2009
Keith S. Whyte Executive Director National Council on Problem Gambling	06/05/2009
Jamie Wiebe Director Centre for the Advancement of Best Practices Ontario Responsible Gambling Council (Canada)	08/07/2009
André Wilsenach Chief Executive Officer Alderney Gambling Control Commission	08/27/2009