Georgetown University

From the SelectedWorks of Mark MacCarthy

October 1, 2009

What Internet Intermediaries Are Doing About Liability and Why It Matters

Mark MacCarthy, Georgetown University

Available at: https://works.bepress.com/mark_maccarty/1/
What Internet Intermediaries Are Doing About Liability And Why It Matters
Mark MacCarthy*
Georgetown University

Abstract: In Who Controls the Internet? Goldsmith and Wu answer that intermediaries control it. Internet service providers, payment systems, search engines, and auction sites provide the infrastructure necessary for Internet transactions. These localized enterprises can be influenced by governments to block illegal transactions. Goldsmith and Wu conclude that this ends the hope of Internet exceptionalists such as Johnson and Post that the Internet would be governed by self-organizing communities of users. In addition, some commentators such as Mann and Belzley suggest that intermediary liability is the right public policy if intermediaries are the least cost avoiders.

In this paper, I examine the policies and practices of the Internet payment intermediaries to see (1) whether there is a need for a public policy requiring intermediary liability and (2) whether the intermediary role really does spell the end of Internet exceptionalism. I examine how the payment intermediaries dealt with Internet gambling, child pornography, controlled substances, online tobacco sales and copyright infringement.

These payment intermediary practices suggest several lessons for public policy. First, regardless of the precise legal liabilities, intermediaries have a general responsibility to keep their systems free of illegal transactions and they are taking steps to satisfy that obligation. Second, least cost avoidance is not the right public policy rule, and even if it were intermediaries are not always the least cost avoiders, and even if they were, who pays for their role would still be unresolved. Assessments of intermediary liability have to take into account market failures, as well as analysis of costs, benefits and equities. Third, the subjectivity of the judgments that intermediaries need to make to address illegal transactions argues for a governmental role to clarify the legal issues at stake.

Intermediary practices also illuminate the debate between the Internet exceptionalists and non-exceptionalists. Intermediaries should not themselves defer to the judgments of self-governing communities of Internet users when this conflicts with local law. The ideal of self-governing Internet communities is not refuted by the fact that intermediaries must respond to governments. This ideal could still result from decisions by governments to recognize Internet community norms. Given the failure of the “bordered Internet” recommended by Goldsmith and Wu to scale up, it is worth reconsidering it. But I argue for global harmonization. Many reject it, arguing that it would destroy diversity in favor of a bland universalism. But the intermediary experience suggests that some international harmonization is needed. The practical rule to ban a transaction when it is illegal in either jurisdiction works when the number of jurisdictions involved is small, but will overwhelm any global system as the number grows. Moreover this rule does not work at all where the law of one country requires what the law of another country forbids. If governments are going to use intermediaries to regulate the Internet, they need to coordinate their own laws to make that role possible.

* Mark MacCarthy is Adjunct Professor in the Communications Culture and Technology Program at Georgetown University. Formerly, he was Senior Vice President for Public Policy at Visa Inc.
I. INTRODUCTION

Internet exceptionalists began a fruitful debate in the mid-1990s over the best way for governments to react to the development of the Internet as a global communications medium. Their fundamental insight was that reliance on local governments to set rules for the new online world would not scale well. Their alternative was the notion of cyberspace as a separate place which should be ruled by the norms developed by self-governing communities of users.¹
The response was a vision of a bordered Internet. In this view, cyberspace is not a separate place. It is simply a communications network that links real people in real jurisdictions with other people who might be in different jurisdictions. Governments had many different ways to regulate activity on this new communications network, including reliance on the local operations of global intermediaries. These entities were the Internet service providers, payment systems, search engines, and auction sites that provide the infrastructure necessary for Internet transactions. They were often global in character but they had local operations that were subject to local government control. Governments had the right and the obligation to use this regulatory power over intermediaries to protect their citizens from harm. Conflicts that might arise from this regulatory activity could be resolved in the normal way that governments resolve conflict of law questions.²

Governments followed the advice of the proponents of regulation, not the regulatory skeptics. And despite some set-backs in First Amendment cases,³ they have continued a steady march toward increased use of intermediaries to control the Internet. Some legal scholars argue that this reliance by governments on intermediaries to control unlawful behavior on the Internet is justified because putting the enforcement burden on intermediaries is the least expensive way for governments to effectively assert jurisdiction. The key point is that governments cannot easily find wrong doers on the Internet, but intermediaries can. They are best positioned to monitor their own systems. As Mann and Belzley put it, they are the “least cost avoider.”⁴

The defenders of local government jurisdiction over the Internet and the use of intermediaries as their chosen instrument often rely on historical analogies to buttress their case. Debra Spar developed the thesis that society’s reaction to new technologies follows a predictable sequence of innovation, commercial exploitation, creative anarchy and then government rules. In the innovative stage a new technology is developed, in the second it is used in commercial ventures, in the third there is a tension between the anarchist impulse and the need for commercial order and stability and in the final stage society reaches out to regulate the now mature technology to bring about and maintain the needed stability.⁵ The development of radio is the standard example here, where the initial pioneers thought the ability of the new wireless technology to broadcast information from one point to many made government control difficult and unnecessary and the later commercial enterprises actively sought out government regulation of the spectrum to end the chaos on the airwaves that prevented broadcasters from reaching their intended audience.⁶ In this analysis, the Internet is somewhere between stage three and stage four, where we can expect further regularization of Internet activity under the watchful eye of government.

Many observers thought the Internet exceptionalists had been routed. However, Internet exceptionalism is still widely held⁷ and the notion that government control of cyberspace is both impossible and illegitimate still motivates much discussion of Internet policy.⁸ Moreover, the initial legislative expression of Internet exceptionalism – Section 230 of the 1996 Telecommunications Act – is still on the books. This section provides a safe harbor from indirect liability for what might be called pure Internet intermediaries – those providing Internet access service and other entities in so far as they provide nothing
but services directly related to the Internet. Despite a growing call for revisiting this immunity from liability, it has been extended several times in recent pieces of legislation. The Internet gambling law, which creates liability for other more traditional intermediaries such as payment systems, contains a limitation on liability for pure Internet intermediaries. The recently passed online pharmacy law also contains an exemption for pure Internet intermediaries from a general duty to avoid aiding or abetting unauthorized Internet sales of controlled substances. The adoption of these provisions in recent laws might be just Section 230 on automatic pilot, but some version of Internet exceptionalism seems to be at work in these legislative distinctions.

For these reasons, it is worth revisiting the debate in light of the experience that Internet intermediaries themselves have had in controlling Internet content. Most Internet intermediaries have explicit policies that prohibit illegal activities. These general policies are supplemented with specific policies and procedures designed to prevent the use of these systems for specific illegal activities. I focus on the traditional payment intermediaries, the payment card companies such as Visa, MasterCard and American Express. Developments over the last several years conclusively demonstrated that these payment intermediaries can control specific Internet activities and that governments can control these intermediaries. I will examine the experience of Internet payment intermediaries in the areas of Internet gambling, child pornography, controlled substances, online tobacco and online copyright infringement to illustrate this point. If the Internet exceptionalists rested their case on the literal impossibility of extending local law to cyberspace then there is not much left of their argument.

But the debate rapidly shifted from the “nature” of the Internet as something intrinsically beyond the control of governments to a problem of choice. Governments can control illegal behavior on the Internet. But should they? Should intermediaries be their chosen instrument? How should the global legal order be structured to accommodate their role?

I try to address these questions in what follows. In Part II, I outline the policies and practices of payment intermediaries in selected areas: Internet gambling, child pornography, controlled substances, online tobacco and copyright. In part III, I develop a framework to analyze the issues raised by imposing indirect liability on intermediaries and apply this framework to the five cases. I conclude that the least cost arguments that are often used in this area are unconvincing: it would be legitimate to create an enforcement role for Internet intermediaries only after a thorough analysis that includes an assessment of market failure, and an analysis of the costs, benefits and equities involved. In part IV, I revisit the Internet governance questions raised by the Internet exceptionalist debate, and reject the vision of the bordered Internet on the exceptionalist grounds that it will not scale well. In contrast to the exceptionalists, however, I conclude that some form of internationalism is the best way forward.
II. PRACTICES OF PAYMENT INTERMEDIARIES

Payment intermediaries have evolved policies and practices to deal with illegal Internet transactions in their payment networks. In this section, I review some of these practices in order to see what can be learned from them regarding the appropriate role of intermediaries in controlling illegal Internet activity.

The payment intermediaries I consider are the traditional payment networks such as Visa, MasterCard, American Express and Discover. These enterprises are private, contractual systems that provide a platform linking merchants who accept cards for payment and cardholders who use them to pay for goods and services. Payment systems include unitary enterprises such as American Express and Discover, and independent companies such as Visa and MasterCard that link separate financial institutions into an electronic payment network.\(^\text{12}\)

Payment systems such as American Express link the two sides of the payment card market directly. They issue cards to cardholders and they sign up merchants to accept their payment cards. Independent network-forming companies such as Visa and MasterCard are different. They do not have direct relationships with cardholders and merchants. These relationships are maintained directly by financial institutions that are parts of the payment systems created and maintained by these network companies. Card issuing banks (“Issuers”) provide network payment cards to cardholders. Acquiring banks (“Acquirers”) sign up merchants to accept network payment cards.

In the Visa and MasterCard systems, a payment card transaction involves an authorization message sent from the merchant where the card is being used to the financial institution that provides processing services for the merchant. The message is routed through the network’s communications and computer systems to the bank that issued the card to the customer. The issuing bank authenticates the card information submitted in the message and authorizes the transaction after ascertaining that the cardholder has sufficient funds or credit. In the case of credit card transactions, sometime after the initial authorization of the transaction, a second process routed through the network system clears and settles the transaction, transferring funds from the cardholder’s financial institution to the merchant’s account at his payment card bank.\(^\text{13}\)

These financial intermediaries are different from pure Internet intermediaries. Pure Internet intermediaries such as Internet access providers, search engines, online auction sites and the like do not have a separate existence apart from the Internet service or application that they provide.\(^\text{14}\) In contrast, payment intermediaries evolved offline. Their primary application is for face-to-face retail transactions; they have extended this primary service to other channels such as mail order or telephone order service. For them, the Internet is just another channel of commerce.\(^\text{15}\)

One of the lessons that can be learned by examining the policies and practices of the traditional payment intermediaries is the extent to which control over the Internet can be exercised by companies that are not themselves intrinsically tied to the Internet.
related policy question is the extent to which exemptions from indirect liability that have been thought to apply to pure Internet companies should also extend to these traditional payment intermediaries that provide essential electronic commerce functionality.

A. Internet Gambling

One of the earliest examples of government efforts to control Internet activity is Internet gambling and its history is rich with lessons. Other commentators have noted the early efforts of government to use financial intermediaries to restrain Internet gambling. But these efforts came from state and federal law enforcement officials trying to use their existing resources to pressure financial institutions to take steps against Internet gambling merchants. For instance, in 2002, Elliott Spitzer, then Attorney General for New York, pressured Citigroup and other financial institutions into agreeing to block Internet gambling transactions.\(^16\)

I want to focus on the more recent national legislation designed to impose a system of indirect liability on financial institutions for the purpose of preventing illegal Internet gambling transactions. Internet gambling was one of the first areas where U.S. national lawmakers became concerned about the way the Internet created a difficulty in enforcing local laws. Many state laws made Internet gambling illegal and Federal law also appeared to outlaw it in interstate commerce.\(^17\) But customers could evade these local laws by visiting Internet gambling merchants located outside U.S. jurisdiction. Early legislation targeted ISPs to require them to stop illegal Internet gambling.\(^18\)

The public policy approach finally adopted was to attach obligations to the financial intermediaries who processed payments involving Internet gambling. This was thought to be feasible, both technically and politically. But the initial way that these obligations were formulated was not feasible. It required financial institutions to stop processing payments for illegal Internet gambling websites.

This was too broad for several reasons. First, the Internet gambling website was normally located in a jurisdiction where Internet gambling was legal. On what basis could a financial institution deny them all access to payment services? Surely the problem was on the buyer’s end, not on the merchant’s side. Second, in many cases, the customers were in jurisdictions where Internet gambling was legal. Here both parties to the transaction seemed to be in conformity with local law. On what basis could payment services for all the activities of the website be denied when at least some, and perhaps the majority of their transactions were legal in both the jurisdiction of the merchant and the jurisdiction of the customer?

The payment networks devised a solution to this issue. Each merchant in the payment system is normally required to identify its major line of business and to include a four digit “merchant category code” in each authorization message. For gambling, the merchant category code was 7995. In addition, merchants were required to identify the channel of a transaction in the authorization method by using an electronic commerce indicator when an Internet transaction was involved. Putting together these two pieces of
information in the authorization message meant that a transaction involving an Internet gambling merchant could be identified in real time by the payment network that transmitted the authorization message or the issuing bank that received it.\(^\text{19}\)

Given this technology, it was clearly feasible for the issuing bank or the payment network to block Internet gambling transactions. The system could accommodate the conflicting laws in the area in the following way: if it was illegal in one country, such as the United States, for cardholders to engage in Internet gambling, then the issuing banks based in that country could decline authorization requests for all properly coded Internet gambling transactions. This would effectively block these transactions. However, the banks in other countries, such as the United Kingdom, where Internet gambling was permitted, could allow the use of their cards for Internet gambling by not setting their systems to decline properly coded Internet gambling transactions.

This system was a reasonable accommodation to the conflicting laws in different jurisdictions, but it was not perfect. For one thing, banks were able to issue cards outside of their own jurisdiction. A British citizen could obtain both a card issued by a U.S. bank and a card issued by a British bank. One card would work for Internet gambling. The other would not. People residing in countries where Internet gambling was illegal would be able to evade payment system blocking by obtaining cards issued by banks from jurisdictions where Internet gambling was legal. This loophole was likely to be small and apply most to ex-patriots who did not give up their local cards when then moved to a new jurisdiction.

A second way in which the blocking system fell short was in regard to Internet gambling by travelers. If I go to Las Vegas, I can gamble there, even though it is not legal to do so in Washington DC. If I go to Great Britain where Internet gambling is legal, I should be able to engage in Internet gambling while I am there. But if I have only a payment card issued by a U.S. bank, I won’t be able to use it because the system is set to decline all properly coded Internet gambling transactions using cards issued by that bank, even those transactions that take place entirely within jurisdictions where the gambling is legal. These “in-transit” transactions, however, were likely to be few, and this seemed to be a relatively small price to pay for a system that largely mapped the major contours of the Internet gambling problem.

The third way in which the system was limited was in detected illegal versus legal Internet gambling. If a jurisdiction recognized some Internet gambling transactions as legal and others as illegal, the system would not detect that. The merchant category code described a type of business, not the legal status of the transaction involved. If sports betting was illegal, but casino gambling was not in a particular jurisdiction, they would nevertheless both be categorized labeled 7995, and if the system was set up to block these coded transactions, then both transactions, the legal and the illegal, would be blocked.

So the industry coding and blocking system would both under block and over block. It would allow some transactions that it should stop such as transactions using cards issued in jurisdictions where Internet gambling was allowed. And it would block
some transactions that it should allow such as transactions that were legal in the jurisdiction in which they took place. Yet it seemed a reasonably good fit to the problem.

The Achilles heel seemed to be enforcement. If an Internet gambling merchant realized that his transactions would be blocked in a large jurisdiction such as the U.S., then it would have every incentive to hide. Instead of describing himself as a gambling merchant, he would just code himself as a T-shirt sales site or some other legal merchant. Without the proper merchant category code, the system was blind and could not effectively block.

The payment networks addressed this enforcement issue with a special program to make sure that Internet gambling merchants coded their transactions correctly. Using public data on the size of Internet gambling sites, payment network personnel would test transactions at the most popular sites. They would enter a transaction at the web site and track the transaction through the payment system. They would be able to tell whether the transaction was coded properly or not after they identified the transaction in the system. If it was not properly coded, the network would contact the bank that worked with the merchant and tell them that their merchant was out of compliance with the coding rule, and ask them to take steps to bring the merchant into compliance. The site would then be re-tested to make sure that the transactions were properly coded.

There was nothing automatic about the coding enforcement program. Human beings entered the transactions, tracked them in the processing and authorization system, found the appropriate financial institution, made calls and sent emails to that institution. It was time consuming and staff resource intensive. And it would be never-ending - if the coding enforcement program were publicly abandoned, the blocking scheme would no longer be effective since the intended targets of the blocking would simply miscode to avoid the blocking.

There was one other way in which a payment system could react to the concern about Internet gambling. That was to avoid signing up gambling merchants. American Express, for instance, refused to sign up these merchants partly because of the substantial risk of non-payment for gambling debts, partly because of legal risk and partly because of the reputational damage involved in accepting transactions that many viewed as sinful or harmful. They too had an enforcement program, which relied heavily on complaints.

The Internet gambling legislation that ultimately became law in 2006, called the Unlawful Internet Gambling Enforcement Act of 2006, (UIGEA) largely tracked this industry system. It created an obligation on payment systems to have in place policies and procedures reasonably designed to stop illegal Internet gambling transactions or as the implementing regulations put it to “establish and implement written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit…” illegal Internet gambling transactions.

The statute creates a safe harbor for payment systems that adopt a coding and blocking scheme. The Federal Reserve Board and the Department of the Treasury implemented this safe harbor with a non-exclusive description of one way in which a
payment system can demonstrate that its policies and practices are reasonably designed to stop illegal Internet gambling transactions:

(ii) Implementation of a code system, such as transaction codes and merchant/business category codes, that are required to accompany the authorization request for a transaction, including -

(A) The operational functionality to enable the card system operator or the card issuer to reasonably identify and deny authorization for a transaction that the coding procedure indicates may be a restricted transaction; and

(B) Procedures for ongoing monitoring or testing by the card system operator to detect potential restricted transactions, including –

(1 ) Conducting testing to ascertain whether transaction authorization requests are coded correctly; and

(2 ) Monitoring and analyzing payment patterns to detect suspicious payment volumes from a merchant customer; 23

To take advantage of this safe harbor, a payment system must, in effect, maintain the coding and blocking scheme that was in place around 2006. Of course, other ways to satisfy the general duty are possible, but the presence of an approved safe harbor written into both statute and implementing regulations puts a substantial burden on any replacement mechanism to be demonstrably at least as effective as the approved safe harbor. The practical effect of this is to extend the current payment system coding and blocking system into the indefinite future.

A key issue in the implementation of the law was the question of clarifying the status of certain gambling operations as legal or illegal. A discussion of this issue illustrates an important point that will emerge in other areas as well: providing for private sector enforcement of legally ambiguous laws creates significant problems for the intermediary and for other market participants who are affected by the legal ambiguity.

The Act generally defines “unlawful Internet gambling” as placing, receiving, or otherwise knowingly transmitting a bet or wager by any means which involves the use, at least in part, of the Internet where such bet or wager is unlawful under any applicable Federal or State law in the State or Tribal lands in which the bet or wager is initiated, received, or otherwise made. The Act states that its provisions should not be construed to alter, limit, or extend any Federal or State law or Tribal-State compact prohibiting, permitting, or regulating gambling within the United States. The Act does not spell out which activities are legal and which are illegal, but rather relies on the underlying substantive Federal and State laws 24
The Federal Reserve Board and the Department of the Treasury (the Agencies) reasonably refused to try to define the unlawful Internet gambling. “After consulting with the Department of Justice and representatives from the offices of several State attorneys general regarding this issue, the Agencies have determined that a single, regulatory definition of "unlawful Internet gambling" would not be practical. The Act's definition of "unlawful Internet gambling" relies on underlying Federal and State gambling laws. The States have taken different approaches to the regulation of gambling within their jurisdictions and the structure of State gambling law varies widely, as do the activities that are permitted in each State. Accordingly, the underlying patchwork legal framework does not lend itself to a single regulatory definition of "unlawful Internet gambling."”

The difficulty of the issue can be seen in regard to horse racing. Existing statute appears to authorize Internet betting on horse racing. The Interstate Horseracing Act (IHA) authorizes interstate off track wagers and then defines this term as:

“…a legal wager placed or accepted in one State with respect to the outcome of a horserace taking place in another State and includes pari-mutuel wagers, where lawful in each State involved, placed or transmitted by an individual in one State via telephone or other electronic media and accepted by an off-track betting system in the same or another State, as well as the combination of any pari-mutuel wagering pools.”

The facial meaning of this definition seems to allow bets on horseracing to take place through electronic media such as the Internet provided the transaction would be legal in each State. Of course, only domestic providers of these betting services can participate in this type of Internet gambling because only they are located in one of the states. This was the heart of the WTO ruling that the United States Internet gambling laws violated its trade commitments – in effect, U.S. law discriminated against offshore commercial establishments by allowing domestic companies to provide betting on horse racing while prohibiting offshore websites from doing so. Yet the U.S. defense to the WTO complaint alleged that the IHA did not constitute an exemption from the existing laws on remote gambling. Although it was a later statute, it did not explicitly state that it was overriding the earlier statute, and, they argued, a later civil law can override an earlier criminal law only by explicitly stating that it is doing so. The U.S. Justice Department maintains that Internet horse race betting is illegal.

There is no good resolution of this issue for the financial institutions involved. If they block Internet horse racing bets they appear to be siding with the Department of Justice’s interpretation of the law, against the views of the horse racing industry and the WTO. If they do not they appear to be defying the agency charged with enforcing that law.

This left the determination of legality to the payment systems. Card systems were permitted to continue using the industry gambling code as a way to implement the safe harbor. This could result in the blocking of some transactions that industry participants feel are perfectly legal. Financial institutions were generally instructed to resolve all questions of ambiguous legality by following a process of “due diligence” where they
would be required to consult the various state and federal statutes to determine if a particular business was engaged in unlawful Internet gambling.\textsuperscript{32}

The legislation imposed indirect liability obligations on other parties in addition to financial institutions. The law allows the Attorney General or a state AG to ask a district court to enter a restraining order or injunction against any person to prevent or restrain an unlawful Internet gambling transaction.\textsuperscript{33} But these actions are limited in the case of interactive computer services. The remedy can only ask the computer service to remove or disable access to a site (or link to a site) involved in illegal Internet gambling. It has to specifically identify the location of the offending site or link. It must apply to a specific service (not to all interactive computer services generally) and the remedy cannot require the service to monitor its system for illegal Internet gambling sites.\textsuperscript{34} We see here an example of the way in which pure Internet intermediaries are treated differently from the traditional payment systems.

\textit{B. Child Pornography}

Internet intermediaries have explicit policies against child pornography.\textsuperscript{35} How do payment systems implement this zero-tolerance policy? The technique of using a code to block the transactions doesn't work at all. Internet gambling establishments are legal in some jurisdictions. So if a merchant electronically labels himself as an online gambler in the payment processing system, he can still engage in the business in those jurisdictions where it is legal. But child pornography is illegal just about everywhere. A self-described child pornography site would instantly be removed from any payment system. Labeling is a mechanism that can be used to accommodate a kind of legitimate diversity of laws in different jurisdictions. But when this diversity is lacking, payment system codes are useless.

Payment card networks work closely with law enforcement to remove any merchants in their systems that are involved in child pornography. But they also actively screen merchants and monitor their systems for this illegal activity without a legal compulsion to do so and without waiting for complaints from law enforcement or other third parties.

Card payment systems enforce their prohibition against child pornography with a two part program.\textsuperscript{36} The first is a set of due diligence requirements designed to prevent child pornography merchants from entering the payment systems to begin with. The second is a monitoring program to detect and expel from their systems any child pornography merchants that manage to fraudulently enter the systems.

The card systems require financial institutions that are part of their network to ensure that all merchants are properly qualified to accept payment cards. This normally involves a determination that a prospective merchant is financially responsible, and will abide by system requirements and applicable law. There are a variety of methods that
financial institutions may use to determine these qualifications, including credit reports, business financial statements, and income tax returns, conducting physical inspections of the business premises of a prospective brick and mortar merchant, and for electronic commerce merchants obtaining a detailed business description and examining the merchant’s Web site.

By taking these precautions, financial institutions can provide a line of defense against child pornography merchants entering the payment system. These due diligence requirements are closely observed by financial institutions, but they are not a panacea for addressing the problem. Child pornography merchants do not present themselves as such to acquiring financial institutions. They often appear to be legitimate merchants. They use a variety of techniques to fool financial institutions, and thereby gain access to the payment systems, despite the best efforts of these financial institutions to screen them out.

Accordingly, the payment systems supplement these due diligence requirements with an active monitoring system. Visa and each of the other traditional payment networks maintain separate monitoring campaigns to identify and eliminate transactions emanating from child pornography merchants. Visa’s program, for example, began in 2002. It has retained the services of an outside firm to search the Internet for child pornography websites that appear to be accepting Visa payment cards. This firm uses advanced web crawling and filtering technology to detect these websites. It looks for websites that display the Visa logo, and that satisfy one or more indicators that they are engaged in the sale of child pornography or are marketing themselves as engaged in that business. The sweeps are ongoing; they are conducted daily and search hundreds of millions of web pages each month.

It is important to emphasize that the payments systems are in no better position than anyone else to detect child pornography sites that appear to use their payment systems. Any party could do this. Nothing internal to the system identifies a transaction as a child pornography transaction.

The payment systems do the monitoring themselves because it helps them take the next step, which is determining which of the apparently active websites using payment cards are actually accepting the cards for transactions. When the outside search firm detects one of these problematic sites, they conduct test transactions to see whether in fact the site is accepting the brand’s cards or whether they are merely illegally using the trademark on their site. The search firm tells the card network immediately if they find a site that is accepting their cards for these transactions. Unless requested by law enforcement to leave these sites open, the network then contacts any financial institution found to be processing these child pornography transactions and directs them to stop processing these transactions immediately. If they have not done so within 7 calendar days, they are fined.

If these identified sites are not in fact accepting the payment cards, but are merely using the trademark on their site, the network uses its best efforts to locate the web
hosting company to direct them to remove the logo. In addition, the payment networks Visa provide information regarding all these sites to U.S. and international law enforcement officials and to the National Center for Missing and Exploited Children. At their request and as part of an ongoing law enforcement investigation, the networks Visa would allow these problematic sites to remain operational.

The size of the problem and the effectiveness of the payment card campaign against them can be seen from some industry statistics. For instance, in August of 2006 the search firm working for Visa examined over 11 million Internet sites a day and found two child pornography sites that accepted Visa cards. Since the beginning of 2006 nine such sites had been identified. All of these sites were quickly expelled from the Visa system.  

These individual efforts against child pornography have been supplemented by collective action. In July 2005 Senator Richard Shelby, then Chairman of the Senate Banking Committee, convened a meeting involving the National Center for Missing & Exploited Children (“NCMEC”), the International Centre for Missing & Exploited Children (“ICMEC”) and key financial industry leaders to encourage the private sector to work together to attack the problem of commercial child pornography. In March 2006, payment systems and financial institutions joined with the national Center for Missing and Exploited children to form the Financial Coalition Against Child Pornography and announced the formation of this group at a press conference attended by Senator Shelby. The group shares information and takes collective action against child pornography merchants identified by complaints to the NCMEC hotline or resulting from Internet searches. This effort has produced some positive results in terms of disruption of the activities of child pornographers and has caused some movement away from recognized payment brands and toward less traditional payment mechanisms.

C. Controlled Substances

All Internet intermediaries take specific extra precautions to protect against the use of their systems for traffic in controlled substances. Payment systems treat controlled substances in a fashion similar to the way they addressed the problem of child pornography. They have a proactive policy of screening merchants and monitoring transactions to prevent the use of their systems for transactions involving controlled substances. They distinguish controlled substances from other prescription drugs and take special precautions to ensure that websites selling controlled substances without proper authorization are expelled from their system, while other legitimate Internet pharmacies are allowed to function normally.

Payment systems efforts to prevent the use of their networks for transactions involving controlled substances were developed in conjunction with U.S. law enforcement agencies. In 2004 and 2005, payment systems representatives met with the Food and Drug Administration and with the Drug Enforcement Administration to develop strategies to deal with the problem of the sale of controlled substances on the
Internet. The health and safety risks associated with these transactions and the likelihood that these dangerous pharmaceuticals could be obtained by minors led the networks to take active steps.

Coding the nature of the transaction so that financial institutions could block it would not work to address the problem of controlled substances. The only codes available identified the business of the website, but not the nature of the pharmaceuticals dispensed. Many legitimate websites sold pharmaceuticals under appropriate government regulation and private sector oversight. If the business code were used as a trigger to block these transactions, the result would have been to eliminate a substantial and desirable Internet business.

The only effective approach was a program of due diligence supplemented by an active monitoring program. Payment systems refined these programs in cooperation with the FDA and DEA. For example, as part of its due diligence program in 2004 and 2005, Visa reminded affiliated financial institutions of their responsibilities to ensure that only legal transactions enter the Visa system and directed their attention to the lists of controlled substances and problematic drugs maintained at the FDA and DEA websites. Visa also directed its members to the FDA public safety bulletins on the FDA website on buying medicines online and noted that a safe website should be licensed by the state board of pharmacy where the website is operating, have a licensed pharmacist available to answer questions, require a prescription from a U.S. licensed doctor or other healthcare professional licensed in the U.S. to write prescriptions and provide a way to speak to a person about problems. Visa also advised its members to consider relying on a reputable seal program, such as the Verified Internet Pharmacy Practices Site Program ("VIPPS") operated by the National Association of Boards of Pharmacy, as a means of identifying reputable Internet pharmacies. When alerted that specific Internet pharmacies may be accepting Visa cards for illicit transactions, Visa worked to investigate these pharmacies and to terminate the acceptance of Visa cards for illicit activity.

As in the case of child pornography, these due diligence efforts are necessary but not sufficient. The payment networks separately retained the services of an outside firm to search the Internet for websites selling controlled substances and accepting their payment cards. This program builds on the program for monitoring the Internet for child pornography, uses the same web crawling and filtering technology, and the same outside search firm to conduct the Internet sweeps. This vendor looks for websites that display the card brand’s logo, that sell Schedule II controlled substances or other prescription drugs that the FDA or DEA have indicated are especially dangerous, and that do not require a prescription or an exam. The sweeps are ongoing; they are conducted daily and search hundreds of millions of web pages each month. The networks then take steps to remove their merchants who appear to be involved in selling controlled substances.

These efforts have produced positive results. In 2005, MasterCard indicated that they had located and shut down 500 websites selling illegal controlled substances. The National Center on Addiction and Substance Abuse (CASA) at Columbia University has studied the nation's problem of controlled prescription drug abuse and has documented
the Internet availability of these drugs. Its early reports described what looked like a steady increase of the availability of controlled substances. In 2008, however, it documented a decline in the number of websites advertising or selling controlled substances, and suggested that this decline could be attributed to financial service company efforts to block controlled substance transactions.

D. Online Tobacco

Sales of tobacco products online are controversial for many reasons, including the inability to control sales to minors. For this reason, many Internet intermediaries restrict the way their systems can be used in connection with online tobacco sales.

A series of coordinated steps by the Bureau of Alcohol, Tobacco and Firearms (BATF) and the state attorneys general in 2004 and 2005 led to changes in the way payment intermediaries processed online tobacco sales. These efforts by state and federal law enforcement officials were not couched as demands to end illegal action by the intermediaries themselves. Rather the idea was that the underlying activity was illegal, and once this was brought to the attention of the intermediaries, they would respond by taking voluntary measures to stop the illegal transactions. Since all payment intermediaries have a general rule against allowing their systems to be used for illegal activity, it seemed reasonable that they would take this step. In fact, almost all of them did.

In January 2005, 42 State Attorneys General wrote to the payment card networks saying that virtually all online tobacco retailers engage in illegal sales. They listed the laws they believed were violated and asked that the payment networks not allow their payment cards to be used to purchase tobacco products over the Internet unless and until a specific retailer can prove that it is not in violation of state or federal laws. They also asked that the networks take appropriate steps to ensure that their credit cards were not used to facilitate violations of state or federal laws.

In January 2005 at a meeting in New York City there were presentations from representatives of BATF and the Office of the Attorney General of New York State to Visa, MasterCard, American Express, Discover, and PayPal. These presentations described the violations of Federal, State and local Statutes involved in the online sale of tobacco products.

In March 2005, the card companies reached an agreement with the state Attorneys General and with BATF to take steps against the online sale of tobacco products. The release accompanying this agreement stated:

Among the many actions the credit card companies have adopted to stop illegal online sales are:
1.) Adopting policies to prohibit the use of credit cards for the illegal sale of cigarettes over the Internet; and, 2.) Agreeing to investigate and take action with
respect to any Internet sellers identified by law enforcement agencies as using credit cards for illegal online cigarette sales.  

MasterCard reacted by sending a notice to their member banks requiring them to cease card acceptance for Internet tobacco, or prove to the satisfaction of BATF and the relevant State Attorneys General that they are in compliance with relevant laws. Visa responded as well by sending a notice to its membership, reproducing the letter from the State Attorneys General, reminding them that they must ensure their merchants are in full compliance with all state and federal laws and be prepared to demonstrate that to law enforcement upon request. Unlike the case of child pornography and controlled substances, however, the payment networks relied on complaints from law enforcement to direct their efforts to stop the illegal activity. As a result of these steps the number of online tobacco merchants decline dramatically. They estimated that they had cut off the 100 largest online sites.  

In addition, the state Attorneys General sought and obtained the cooperation of the carriers that delivered cigarettes from online tobacco stores to purchasers. In July 2005 DHL agreed not to deliver cigarettes for illegal Internet sellers. In October 2005, UPS agreed to stop shipping cigarettes to consumers throughout the United States. In January of 2006, FEDEX agreed to stop shipping cigarettes from online stores. The U.S. Postal Service rejected the request to stop delivering cigarettes from online tobacco stores, citing federal requirements that it deliver the mail. One response was the introduction of legislation to require the Postal Service to stop deliveries.

This case also shows how payment systems other than card systems have a role to play in stopping illegal transactions on the Internet. In July, 2006 the State Attorneys General followed up with requests to NACHA, the association responsible for managing the Automated Clearing House (ACH) to cease processing transactions involving Internet tobacco sites. Their letter cited the legal problems associated with online tobacco sites:

“…virtually all Internet tobacco retailers engage in illegal sales for at least one of the following reasons: (1) they make no effort to verify the age of their customers, as required by state and local laws; (2) they violate the federal Jenkins Act (15 U.S.C. §375 et seq.) by failing to report shipments of cigarettes to the tobacco tax administrator of the state into which such shipments are made; (3) they violate laws in certain states specifically prohibiting or regulating the sale of tobacco products over the Internet; (4) they violate state tax laws; and/or (5) they utilize the Internet and the mail to complete illegal tobacco transactions, in violation of federal wire fraud and mail fraud statutes.”

In response, NACHA sent an operations bulletin to its members strongly encouraging them “to establish business practices that ensure that ACH transactions do not facilitate illegal activity.” It strongly warned its members that they could be liable for facilitating these illegal transactions.
In May 2008, Christopher K. Leung, from the New York State Office of the Attorney General, briefed the NACHA Payments Conference on Internet Tobacco Sales and the ACH Network. In his presentation, he warned that online tobacco sites typically violate the Jenkins Act, the Federal Cigarette Excise Tax Law, the Contraband Cigarette Trafficking Act, the Mail and Wire Fraud Acts, the Counterfeit Stamps and Cigarette Laws, the Money Laundering Laws, and the RICO Act. He noted that with the agreements from the payment card companies, “Internet tobacco retailers have moved almost exclusively to the ACH network.” He warned of potential legal liability for banks that allowed the ACH to be used for online tobacco sales, and urged banks to “refuse to service Internet tobacco retailers.”

In 2006, the Attorneys General from Iowa, New York and California began investigating whether the activities of some Internet tobacco retailers were in violation of state laws. In 2007 they looked into the activities of First Regional Bank to determine whether the bank was facilitating illegal online tobacco sales. In early 2008, the bank discontinued any processing services for online tobacco retailers. In September 2008, the bank and the state Attorneys General reached a settlement under which the bank agreed not to providing services to online tobacco merchants and to discontinue services to any merchant found to be involved in online tobacco sales. In addition, they agreed to a program of due diligence under which they would investigate prospective merchants to ensure that none were online tobacco merchants and would re-investigate them from time to time.

The state Attorney General continued to put pressure on payment intermediaries in regard to their provision of service to online tobacco retailers. An electronic payment process called the Electronic Clearing House (ECHO) bundles payments by merchant customers and submits them to the Automated Clearing House Network or to the credit card networks for electronic payment processing. ECHO was providing these services to a number of online tobacco retailers. The states Attorneys General from California, Iowa and New York determined that ECHO was facilitating illegal online tobacco sales by processing for these online tobacco retailers. In December 2008, ECHO and these state Attorneys General reached a settlement under which ECHO agreed not to process transactions from online tobacco retailers.

There is no specific statute that makes it illegal to provide payment services or other intermediary services to online tobacco retailers. But there are general requirements to avoid facilitating illegal transactions. The request from law enforcement to aid in the fight against online tobacco sales was thus backed by an increase in legal risk if they did not. In addition, while there was no implication that intermediaries had to actively screen their systems for illegal tobacco sales, the way they had voluntarily undertaken in the case of child porn and controlled substances, the due diligence requirements imposed in the settlements suggested that some degree of system screening would be necessary to reduce the risk of a facilitation charge.

**E. Online Copyright Infringement**
When payment intermediaries took steps against Internet gambling merchants, child pornographers, purveyors of controlled substances and online tobacco merchants they were acting together with law enforcement officials. The information they gathered in the searches of their systems were provided to law enforcement. They reacted to complaints brought to them by law enforcement agencies. With copyright cases, the complaining party was a private party alleging that some other party had harmed them by infringing on their copyright.

On the face of it, this is very awkward place for intermediaries to be. Private parties are in a dispute about their respective rights under the law. No adjudication has been made of the merits of the case. In some cases, no legal assertion of rights has been made at all to the allegedly infringing party. Why should another private party simply take one side of the dispute, and use whatever relationship they have with one of the parties to enforce the other party’s rights? How should they know who is right? And if they do take action and get it wrong, why wouldn’t the aggrieved party pursue them for taking wrongful action against them?

The ideal would be for copyright owners to sue direct infringers. But direct infringers are sometimes too ubiquitous, too small or too difficult to find. As a result, there are well-developed notions of secondary liability for infringement of copyright that crucially involve intermediaries. These doctrines of secondary liability have evolved substantially over the past decades.

The 1984 Supreme Court decision in Sony v. Universal City Studios established a standard for assessing third party liability in this area. Providers of a technology that can be used for infringing activities are not liable when there are “substantial non-infringing uses” of the technology. The Digital Millennium Copyright Act of 1998 enabled copyright owners to enforce their existing rights in the Internet context by enlisting the help of Internet intermediaries in actions against copyright infringement. The key mechanism was a safe harbor from secondary liability. Internet service providers were given an exemption from secondary liability in so far as they were acting as a pure conduit, providing only transitory communications and system caching. Web hosts and search engines also received a safe harbor provided they complied with a specific notice and take down procedure - upon receiving proper notification of claimed infringement, the provider must expeditiously take down or block access to the material.

Successful litigation against peer-to-peer networks in the digital music area also increased the ability of copyright owners to use third parties to combat copyright infringement. The recorded music industry sued peer-to-peer companies for secondary infringement, and won. In August 2000 a District Court decision granted record companies an injunction stopping Napster’s activities. It ruled that Napster users are direct infringers, and that Napster itself was guilty of secondary infringement. In February 2001, U.S. Court of Appeals for the Ninth District upheld the district court decision barring it from providing its service, and Napster went out of business in its original form.
Grokster was a more difficult case because it did not have a central computer that controlled the peer-to-peer network. A district court decided in April 2003 that Grokster was not guilty of secondary infringement. This was upheld by an appeals court in August 2004, but the Supreme Court reversed the lower court decisions and found Grokster guilty of secondary infringement. In June 2005 the Supreme Court ruled that peer-to-peer software developers and other technology vendors may violate federal copyright law when they take "affirmative steps to foster infringement by third parties."66

Against this background, there was a question regarding payment systems: were they involved in secondary infringement when their payment systems are used for direct infringement? The key case is Perfect 10 v. Visa.67 Perfect 10 operated a subscription adult-content website. It alleged that numerous websites based in several countries had stolen its proprietary images, altered them, and illegally offered them for sale online. In response to complaints, Visa had not denied payment services to these allegedly infringing sites. Perfect 10 then brought a contributory and vicarious infringement action against Visa. The district court and then the Ninth Circuit rejected liability for Visa. The Supreme Court did not take up the case.

The Ninth Circuit dismissed the charge of contributory infringement, focusing especially on whether the card companies “materially contributed” to the infringement. The court said they did not materially contribute to the infringement because they had no “direct connection” to the infringement. To have direct connection to the infringement they would have had to reproduce, display or distribute the allegedly infringing works, which they did not do. Payment services might make it more profitable to infringe, but they are too far removed in the causal chain that leads to the actual infringing acts for them to be described as materially contributing to it.

The Court made a similar point with respect to vicarious liability. The card companies had no practical ability or right to prevent the infringing activity itself. They can exert financial pressure on the infringing websites, but they cannot stop the actual reproduction or distribution of the infringing images.

In his dissent, Judge Kozinski rejected both arguments. He said that the card companies are directly connected to the infringement because they provide payment services and without payment services there would be no infringement. They had the contractual right to terminate illegal activity on their systems and by exerting financial pressure they had the practical ability to stop or limit the infringing activity.

1. Payment System Complaint Program

Even if payment intermediaries are not required by current law to take steps against online copyright infringement, they have chosen to do so.68 They go beyond their legal requirements for a variety of business reasons. The association of payment systems with illegal activity is harmful to their brands. It is good for their reputation as a responsible business partner to react favorably where possible to complaints by reputable
businesses of substantial financial losses associated with illegal activities. It lends credence to their oft-repeated assertions that their payment systems should not be used for illegal activities. By keeping electronic commerce free of illegal activity, the payment networks promote a channel of commerce where they have a competitive advantage over other traditional payment mechanisms like cash and check.

How did payment systems take on the challenge of responding to complaints of copyright infringement? Payment systems cannot monitor their networks for violations of copyright. They simply do not have the factual basis to conclude that a particular sale of a product is a violation of someone’s copyright. Many music downloads are perfectly legal transactions. Some are not. Distinguishing the two is often a complex factual and legal question and payment intermediaries do not have the expertise or ability to resolve these complex questions.

For this reason a coding and blocking system like the one used in Internet gambling will not work. Codes relate to business category, not legal status. If financial institutions blocked transactions based on the business code for a music download, they would block substantial numbers of legal transactions. Since copyright owners benefit from these legal transactions, they would not want an overly broad coding and blocking scheme.

A coding and blocking scheme would be inappropriate for a second reason. Internet gambling is legal in some jurisdictions and illegal in others. For that reason it makes sense to require merchants to properly code themselves and then allow the financial institutions in the countries where Internet gambling is illegal to block these labeled transactions. But Internet merchants involved in illegal intellectual property infringement are typically violating the laws of most countries. It would be highly inefficient for payment systems to allow a merchant to introduce a transaction into the system when the vast majority of financial institutions in the network would have to program their payment processing operations to reject these transactions.

So the best way to respond to complaints about infringing activity is not to require coding by the infringing merchant, but to prevent the merchant from entering the illegal transaction into the system or to restrict it to those few jurisdictions where it might be legal.

Since the payment systems cannot monitor for copyright violations on their own, they have to react to complaints, not take proactive steps as they could in the case of child pornography or controlled substances. So the payment networks have developed policies and procedures to handle these complaints. These complaints do not involve health and safety, but they pose a business problem for these companies and the payment networks attempt to respond, especially in large magnitude cases.

The process of complaint starts when a business entity approaches a payment system with clear, documented evidence of illegal activity and adequately identifies the infringing Internet merchant. The business entity must provide substantiation that the
activity is illegal and documentation that payment cards are actually being used for this illegal activity.

The next step is an assessment of legality. This is easier if there has been regulatory or judicial decision that establishes the illegality, but this is often not the case. If the buyer and the seller are in the same jurisdiction, this legal assessment can be relatively straightforward. But these cases are not typical because companies tend to pursue domestic remedies for domestic cases. They come to payment networks usually in cross-border cases, involving a merchant in one location and the customer in another. If the legal situation in both countries is the same, the legal assessment can be relatively uncomplicated. But what if the merchant is in one jurisdiction, the customer in another and the laws are not the same or the legal situation in one country is not as clear as the legal situation in the other?

Initially, the payment networks did not want to pursue a case with the merchant if the law of the merchant seemed to allow the transaction. How could a merchant know the laws of all the countries he might be selling into? If there was a problem, it had to be resolved on the customer’s end. But this brought the payment networks back to a coding and blocking scheme, which was unworkable in the case of copyright infringement. Moreover, given the relative uniformity of copyright rules, this policy of putting the burden on the customer’s end meant that merchants in a single outlier county could place enormous burdens on the rest of the system.

After wrestling with these issues, the payment networks developed a policy for cross-border transactions: if a transaction would be illegal in either the jurisdiction of the merchant or the jurisdiction of the cardholder, the transactions should not be in the payment system. In cases like copyright infringement, this meant that merchants were responsible for making sure that the transactions they submitted to the payment system were legal in both the jurisdiction in which they operated and the jurisdiction where their customer was.

The assessment of legality, then, involves a determination by the payment network of whether the type of transaction would be illegal in either jurisdiction. Since the facts and law are often complex, the payment networks are willing to take on only what appear to be the clearest cases of copyright violation. Once illegality is determined, the payment providers do what they reasonably can to assist the complaining party. Since payment networks do not work directly with merchants, they typically try to locate the bank that has the merchant account. Providing the complaint to the bank involved usually resolves the issue. In most cases, the bank does not want the business and terminates the merchant or takes other action to bring the merchant into compliance. If the bank does not take action, the payment networks can take further enforcement action against the bank.

In some cases, the merchant resists payment system enforcement efforts, insists on the legality of the underlying activity and goes to court in the local jurisdiction to
vindicate what it perceives to be its rights under local law. This is what happened in the Allofmp3.com case.

2. Allofmp3.com

In 2005, Visa received a documented complaint by International Federation of the Phonographic Industry (IFPI) which represents the copyright owners based in more than 70 countries, that Allofmp3.com, a website located in Russia, was infringing on the copyrights of their members by allowing downloads of music without having obtained the authorization of the copyright owners. Visa conducted an assessment of the legal situation, including a review by outside counsel, and concluded that the transactions were illegal under local Russian law. They were also illegal under the laws of the vast majority of the merchant’s customers – who were located primarily in the UK and US. In May 2005 a German court granted a preliminary injunction against the site saying that it had no right to offer music in Germany without the proper rights holders' consent. In October 2005 the Italian authorities shut down a portal, allofmp3.it, and began a criminal investigation into it. In addition, the United States Trade Representative intervened with the Russian government to urge them to shut down allofmp3.com.

As part of its general policy on cross-border transactions, Visa concluded that it did not want these transactions of this type – illegal downloads of music - introduced into its payment system. This enabled it to extend enforcement actions against this one site to different sites or to the same site processed by a different bank.

At the beginning of September 2006, after appropriate notice, the Russian bank working with Allofmp3.com stopped processing Visa transactions for Allofmp3.com. At the end of September 2006, the bank also stopped processing transactions from an affiliated download music site called allTunes. After these Visa transactions ended, further confirmation of the site’s illegality seemed to be forthcoming: A Danish court ordered the Internet provider Tele2 to block its subscribers' access to allofmp3.com, thereby making it harder for potential customers to access the site. MasterCard and PayPal also cut off payment services to allofmp3.com, and by May of 2007 its popularity had plummeted.

The company was all but out of business, but the legal process was just starting. The owner of allTunes sued the bank that had stopped processing its Visa transactions in a Russian court. Visa was a party to that litigation on the side of the bank. In June 2007, the owner won a judgment that the bank had violated its contract with the merchant, and the bank would be required to provide processing services. In response to the bank’s claim that the merchant was acting illegally, the court determined that there were no rulings in Russia establishing that allTunes was making illegal use of exclusive rights belonging to some rights holder.

In August of 2007, a different Russian court issued a ruling in a different case, relating to criminal copyright infringement initiated by IFPI against the owner of
Allofmp3.com. This ruling stated that there had not been sufficient confirmation of any illegal activity by the site's owner. Even though the copyright owners had not given permission for the distribution of their recorded material, a Russian collective rights organization (the Russian Multimedia and Internet Society, or ROMS by its initials in Russian) was deemed to be operating legitimately under Russian law. The court implied that this and similar sites would be in compliance with Russian law to the extent that they paid for rights from this Russian collective rights society. 76

These court cases created a challenge for Visa. The payment system had responded to a documented complaint of copyright infringement. Despite an outside review that seemed to establish illegality in the local jurisdiction, a local court ordered a local bank to continue to provide payment services. Yet these transactions would still be illegal in virtually every other country in the world. To preserve its cross-border policy, Visa decided to allow the local bank to provide only domestic service to the site involved in the court case, but transactions from customers in other countries would not be allowed.

III. INDIRECT INTERMEDIARY LIABILITY

A. Indirect Liability Regimes

The previous examples of how payment systems reacted to specific illegal transactions on their systems all involve indirect liability regimes. In this section I develop a framework for analyzing these regimes and apply it to the actions the payment systems have taken and to the actual or potential liability regimes applying to their actions.

An indirect liability regime holds a person responsible for the wrongs committed by another. There are usually several parties involved in an indirect liability regime: the bad actor, the wronged party and a third party. The bad actor is the person directly involved in causing the harm to the wronged party. A third party, neither the bad actor nor the wronged party is assigned the responsibility to prevent the harmful conduct of the bad actor or to compensate the wronged party for the harm. In the copyright example described earlier, the bad actor would be allofmp3.com, the wronged party would be Visa or the other payment networks. 77

Indirect liability can be imposed through a variety of legal mechanisms.78 In a tort damages regime, a third party must pay for harms caused by others either on a strict liability or negligence basis. Employer liability for the harms caused by employees is a standard example. Statute or court decisions can impose liability for monetary damages for specific types of harms. Additionally, statutes can require third parties to take certain specific steps to prevent harms to others. A wide variety of legal structures can be usefully viewed as indirect liability regimes, including data security and notification.
requirements, some privacy requirements, and some consumer protection requirements imposed on financial service companies.

The current regime for intermediaries depends on the intermediary and the legal context. ISPs and others have substantial immunity. The Communications Decency Act of 1996 exempted “interactive computer service providers” from certain kinds of third party liability by determining they are not “the publisher or speaker of any information provided by another information content provider.” The Digital Millennium Copyright Act of 1998 bars indirect copyright liability for ISPs who are acting only as a conduit and limits liability for web hosting and other service providers if they follow a prescribed notice and takedown procedure. As we have seen the recent Internet gambling and online pharmacy laws continue this tradition of immunity.

Payment intermediaries are subject to an indirect liability regime by the provisions of the Unlawful Internet Gambling Enforcement Act. But, according to the Perfect 10 case, they are not liable for copyright infringement occurring on their systems. The new online pharmacy law might subject them to specific aid or abetting liability for online sales of controlled substances.

Online markets appear to be subject to some degree of indirect liability for the sale of counterfeit goods. The district court in the Tiffany v eBay case ruled that eBay has some responsibilities under trademark law to avoid providing its services to sellers when it knew or had reason to know of trademark infringement by those sellers. They satisfied that responsibility by a series of measures including an effective voluntary notice and take down program. That responsibility did not extend, however, to a positive duty to monitor its auction site and preemptively to remove possibly infringing listings. The E-Fencing legislation under consideration in the House would extend indirect liability requirements to online markets for preventing the sale of stolen goods.

B. A Framework for Analysis

Indirect liability holds a party responsible for wrongs committed by another person. Why should there be any such rule? Why not simply hold the bad actor responsible? The economic analysis of indirect liability attempts to answer this question using some standard economic tools and concepts. A standard exposition of this framework begins by examining two conditions under which an indirect liability rule is not necessary and then, assuming that those conditions are absent, moves on to considerations of control and activity level in assessing an indirect liability regime. I will use that account as a basis to construct a broader framework.

1. Market Failure Analysis

Before imposing an indirect liability regime, economic analysis asks first whether there is really any market failure. If there’s no market failure then, there’s no need for an indirect liability rule. In particular, there need not be an indirect liability rule when the
law or the wronged party can effectively reach the bad actor directly\textsuperscript{88} and transaction costs are not significant.

But even if the wronged party cannot easily reach the bad actor, and a third party can, it still is not necessary, from an efficiency point of view, to impose liability on the third party, when the wronged party and the intermediary can easily negotiate an arrangement where the third party undertakes enforcement efforts on behalf of the wronged party. This is a key aspect of a market failure analysis. Unless transaction costs interfere with contracting, affected parties can allocate liability efficiently through contractual design.\textsuperscript{89}

This transaction cost condition has not been emphasized enough. In the case of mitigation of tangible, measurable, financial harm to a wronged party who can deal directly with an involved third party, it is hard to see why it matters from an efficiency point of view whether the law creates third party liability. No matter what party bears the liability, efforts to stop the harm should continue up to the point where further efforts are not worth it, that is, until mitigation efforts cost more than they save. If liability is assigned to the intermediary, then he will take mitigation steps himself or pay the wronged party to do it, whichever is less expensive. If liability is assigned to the wronged party, then he will take the mitigation steps himself, or pay the intermediary to do it, whichever is less expensive. Liability assignments do not change the level of mitigation effort, but change the burden of distribution – in the one case, the intermediary pays, in the other the wronged party. As Coase noted long ago, the allocation of resources is the same, but the equities are different.\textsuperscript{90}

As a practical matter in many cases, wronged parties bear the costs of these harms under today’s legal regime. It is possible that mitigation efforts by intermediaries could reduce these harms. If so, efficient markets should lead wronged parties to create arrangements with intermediaries to take these steps, at least up to the point where further payments to intermediaries did not produce an equivalent amount of reduction in damages.

The processes set up by payment intermediaries to respond to external private party complaints are the beginnings of these arrangements and might grow into fuller productive relationships. The extensive processes used by eBay in connection with trademark violations are also the kind of measures that could be built upon to create efficient enforcement efforts. However, mutually satisfactory enforcement arrangements involving third parties have not emerged to any large degree.\textsuperscript{91}

The \textit{Tiffany v. eBay} case illustrates how this transaction cost perspective might be applied. eBay has a notice and takedown program, described by a senior eBay official as follows:

“When we are notified that a particular item is counterfeit, we are notified by the intellectual property owner, someone that actually has knowledge of that product because it is their product, and often they are able to tell just by looking at the item on our site that it is counterfeit. When they certify to us, under penalty of
perjury, that that item is counterfeit, we immediately remove the item from our Web site.”

Tiffany thought this program was ineffective because the sales of counterfeited products could be completed before this notice and takedown program had a chance to operate. They wanted instead to have eBay screen its customers, especially large volume customers to check on whether their sale items were counterfeit and sued eBay for secondary trademark infringement when these arrangements could not be worked out. But Tiffany could have offered to compensate eBay for the costs involved in the extra enforcement efforts it was requesting. There is no indication of transaction costs preventing negotiations. The fact that they were unable to come to an agreement on compensation despite years of negotiations and discussions suggests that the full costs of these enforcement efforts exceeded what Tiffany was willing to pay. If Tiffany is a rational actor, willing to pay up to the amount that it would cost them to take its own enforcement actions, this suggests that eBay was not the least cost enforcer after all.

A similar point applies to efforts to require eBay to take steps to prevent the sale of stolen merchandise on its website. Congress is considering legislation in this area, and has held several hearings on the topic. eBay has an enforcement program called PROACT and a mechanism to work with aggrieved merchants in connection with stolen merchandise. When an aggrieved party comes to eBay alleging that an item for sale on eBay is stolen, eBay asks for evidence and then conducts an investigation. If it seems that the item is stolen, eBay takes the item down, suspends the seller and notifies law enforcement. The issue appears to be who does the serious investigative work. As a witness for the retailer community put it at a Congressional hearing, “PROACT for eBay is a good first step, but it doesn’t go nearly far enough to... put an affirmative responsibility on eBay to do the work.” If all that is at stake is efficiency and not equity, and the costs of this enforcement program to eBay are worth the benefits in loss prevention for retailers then the companies should be able to work out a voluntary program whereby eBay undertakes these efforts on behalf of retailers.

What is really going on here seems to be an argument over the equities. As we will see, in a larger framework of analysis that takes into account considerations of equity and long-term intangible costs and benefits, there might still be a reason to impose third party liability even when the parties can negotiate enforcement arrangements themselves. But the absence of liability arrangements with third parties when parties can easily and freely negotiate suggests that the wronged party itself does not think third party liability is worth paying for. This implied evaluation by the wronged party should be a relevant factor taken into account in considering whether to impose third party liability.

The idea that parties could work out who takes what enforcement steps without any explicit indirect liability rule also illuminates the informal arrangements that have been worked out between law enforcement agencies and intermediaries with respect to specific illegal activities. Third parties have frequently worked closely together with law enforcement to deter or prevent violations of law. Intermediaries work with federal state and local law enforcement on a variety of issues from fraud to child pornography to
online tobacco sales to controlled substances. The market failure analysis should look to the presence or absence of these arrangements with law enforcement when assessing whether the direct bad actors are beyond the effective reach of the law.

2. Cost Benefit Analysis

In addition to this market failure analysis, indirect liability regimes can be evaluated using traditional economic tools. Lichtman and Posner emphasize two factors as relevant to deciding whether to impose an indirect liability rule. The first is the extent to which the third party is in a good position to detect or deter the illegal activity. This is the “control” factor. The second comes into play when the third party cannot do anything to detect or deter the illegal activity, but imposing liability can reduce the harm by reducing the all of the activity associated with the third party, legal and illegal alike. This is the “activity” factor. Both of these ideas are ways of applying traditional economic thinking to the special case of indirect liability rules.

The first “control” factor has to be further specified not simply as whether the third party is in a good position to detect or deter the illegal activity, but that he is in a better position than the wronged party, or other potentially liable third parties. In this way, we arrive at the “least cost” conception of third party liability.

In the case of intermediaries, the application of this line of thought would be to put the burden of enforcing the law on the party that can stop the illegal transactions at the lowest cost. According to this line of thought, aggrieved parties and enforcement officials face prohibitively high enforcement costs – often because the perpetrators of these illegal acts are individuals or small enterprises, widely dispersed in offshore jurisdictions. On the other hand, it is argued, intermediaries are in possession of substantial information regarding activities on their system, they can detect the illegal transactions easily, they are already global in character and they can stop all or most of the illegal transactions using simple methods. So it seems that it would be efficient to adopt a legal rule assigning responsibility for stopping illegal Internet transactions to intermediaries. As the least cost avoiders, they should be the Internet police.

In a “least cost” framework, the cost to the intermediary itself and to the direct customers of the intermediary must be taken into account. If ISPs or payment systems have to incur costs to monitor their system for illegal content, then their direct customers pay for that. With the price increase, some customers stop using the service or reduce their usage of it. If the service provided is a network service, then the external network effects on other users of the service have to be counted as well. But, according to the least cost idea, when these costs are less than the costs for enforcement activity by the wronged party or by enforcement officials, then liability rests with the intermediary.

This least cost avoider proposal is not advanced as an interpretation of current law. Moreover, some courts have explicitly repudiated this principle as an interpretation of current law. Rather, the idea is that regulators and legislators should assess in some fashion whether third parties might be in a better position than the
wronged parties to take enforcement action and impose liability on them if the answer is affirmative.

This emphasis on costs is desirable in order to create an efficient enforcement regime. If we are spending more to get a given level of enforcement than we need to why not reduce this wasteful spending and use the saved resources for something productive?

But the emphasis on costs is limited. It ignores the benefits of enforcement efforts. The mistake involved is to think that if efforts by third parties provide more enforcement than efforts by the wronged parties than it must be worthwhile for the third parties to take these enforcement steps. So, it is sometimes thought, if it can be shown that third parties can more easily reach bad actors than the wronged parties, then they should be required to do so. But this is wrong. It is always possible to spend more on enforcement and usually spending more will provide some return. The question, from an economic point of view, is whether that extra spending provides commensurate reductions in damages. The least cost rule is not the right decision rule, even in a strictly economic analysis. We move from a “least cost” analysis to a full cost-benefit analysis.\(^{103}\)

This focus on benefits is the place to analyze the “activity” factor mentioned earlier. The activity factor is relevant because the normal activity made possible by a third party imposes an external harm on someone else. Assigning liability for monetary damages for this harm to the third party means that price of the activity it makes possible will rise and this will reduce all of this activity. This in effect internalizes the negative externality that these activities inflict on the wronged parties. The point though is not to provide the third party with an incentive to stop just the harmful activity, but to discourage all of the activity they make possible.\(^{104}\)

This focus on the harms that intermediaries and the users of intermediary products and services would suffer from the imposition of an “activity” tax is an essential feature of any analysis, and deserves to be emphasized in these analyses. The implications of this approach need to be made explicit. Assigning liability to intermediaries, even when they cannot reasonably take enforcement steps to prevent harmful activity, would be justified, on this view, when the overall activity itself causes more harm than good. For example, it would allow us to say, in effect, that there is too much use of the Internet, given the amount of copyright infringement it allows, and so we have to reduce Internet usage. This clarity is helpful in assessing the cost of copyright enforcement: the price of additional copyright protection is that people will use Internet services and applications less.\(^{105}\)

This focus on benefits is sometimes not directly faced in the case of general law enforcement because we don’t want to put a value on the enforcement benefits, such as reduced child pornography or prevention of public health problems from the sale of controlled substances. But in cases of more tangible harm, such as damages from copyright infringement or counterfeiting, a traditional cost-benefit analysis seems more feasible.

Cost-benefit considerations must be long-term and take into account dynamic considerations\(^{106}\). Sometimes is makes sense to put liability to fix a problem on the party
who can best innovate to resolve it.\textsuperscript{107} Immunity from third party liability regimes can also be based on long-term cost-benefit thinking.\textsuperscript{108} A version of the infant industry argument is also relevant in this long-term context. The immunity from liability set out by Section 230 of the Communications Decency Act and in the DMCA eased the online community’s uncertainty over the extent of their liability and helped spur dramatic new investment in the Internet infrastructure and services.\textsuperscript{109}

This long-term analysis might include consideration of what the world would look like if the same indirect liability burden was placed on third parties by other jurisdictions or for other harms and the likelihood that action in this case would cause action in these other cases. The political implications are one aspect of this. Unilateral attempts to use intermediaries to enforce local laws might create substantial international discord and ramifications in other areas of political or economic life. The cost analysis also needs to account for implications for the third party itself potentially burdened with costs from many jurisdictions, which might be individually rational, but collectively unworkable. If the foreseeable result of imposing third party liability will be a “race to the bottom,” for other cases and other jurisdictions, this has to be part of the cost analysis.

Finally, there is a difference between the costs and benefits to the private parties involved and the social costs and benefits. The costs and benefits of third party enforcement efforts fall on different parties. A wronged party benefits from third party enforcement efforts and the third party pays the costs. The wronged party has a natural incentive to have the third party do as much as possible in the way of enforcement – even past the point where there is a corresponding reduction in damages – because the wronged party appropriates whatever damage reduction there is and pays no costs. But from an economic efficiency point of view these enforcement efforts past the point of commensurate reduction in damages are wasted: enforcement efforts have to be reasonable in light of the damages avoided regardless of who gains and who loses. Private benefits may not be worth it from a social point of view when balanced against the costs to other parties.

3. Equity Analysis

What are we to make of this framework so far? A clue that something has been left out arises from the example of an “activity tax” just considered. Why should the decision to reduce all activity associated with third party business not raise questions of fairness, rights and justice? Also, why shouldn’t liability decisions take into account who deserves the benefit of protection from harm and who is at fault or blameworthy for failing to take preventive measures?

Mann and Belzley take a very strong position on this question. They want to abstract from “normative” questions: “…a focus on traditional tort law notions of fault necessarily diverts attention to subjective normative questions of blame and responsibility.”\textsuperscript{110} The worry is that these notions will inevitably tangle policy makers up in difficult causation and responsibility questions and will divert attention from the key

29
issue of who can fix the problem. Who created and maintains the problem is not the key, they think; the crucial factor is who can fix it at the least cost.\textsuperscript{111}

The view that an economic efficiency standard, by itself, is sufficient to create indirect liability is too strong. By focusing on parties who had no part in creating the problem and who are not responsible for the illegal activity, it would put a burden on people who are innocent of any wrong-doing. It seems unfair to put this burden on innocent people who have no part in creating and maintaining the harms. The argument that we should put a burden on innocent people because it is good for the rest of us violates widely accepted moral judgments and will not stand public scrutiny.\textsuperscript{112}

We should put a burden on a person to right the wrongs committed by others only if we think that person is somehow responsible for those wrongs. Determining who is responsible for righting wrongs committed by others is a controversial topic in moral and political philosophy. Libertarians tend to say that people are responsible only to fix the problems that they themselves directly created.\textsuperscript{113} This perspective seems to get some support from tort law decisions that do not require affirmative action to rescue third parties, unless, among other conditions, the danger is created by the actor himself.\textsuperscript{114} Others think we have duties to correct injustices to the extent that we are participants in an institutional framework which produces injustice.\textsuperscript{115} Still others think that we have general positive duties to eliminate harms even when we have no direct role in causing them.\textsuperscript{116}

Ultimately, the analysis of indirect liability cannot abstract from considerations of justice, fairness, and rights. The key factors in this assessment will be those that have been used traditionally in these analyses: directness of the involvement by third parties in activities that lead to harm to another person, an assessment of the degree of harm involved, the knowledge that the third party has or should have about the specific harm involved, what their intentions are, whether they are consciously acting in furtherance of a crime or other illegal act, and so on.\textsuperscript{117} These complicated normative and empirical questions cannot be avoided by a single principle that purports to look at costs and benefits alone.\textsuperscript{118}

There is another reason to look to equity questions. Even in cases where transaction costs are low and parties can negotiate enforcement arrangements that make economic sense to them, we still want to know whether it is fair, just, equitable for one party to bear the cost. Distribution matters, not just efficiency. In fact, when courts are looking at cases, like the eBay case, where apparently there are no barriers to efficient enforcement arrangements, the major issues left for the court to decide are these equity questions.

Many who analyze indirect liability questions from an economic point of view recognize that economic considerations are not the only ones. As Lichtman and Posner say: “These factors—call them “control” and “activity level”— are neither alone nor together sufficient to justify the imposition of an indirect liability rule. Instead, these are merely prerequisites that help to identify cases where liability might be attractive. The
actual question of whether liability should be imposed typically turns on other, often setting-specific considerations. They note for instance that a rule imposing liability on telephone companies for crank calls would raise separate privacy concerns that might override the control that telephone companies have in that area.

Because the economic argument is not sufficient on its own to justify indirect liability, it is usually supplemented with the language of blame. The Kozinski dissent in Perfect 10 is an excellent example of this reasoning:

The weak link in the pirates’ nefarious scheme is their need to get paid; for this they must use the services of legitimate financial institutions. If plaintiff’s allegations are to be believed, the financial institutions (defendants here) collect billions for sellers of stolen merchandise; in a very real sense, they profit from making piracy possible. I can see no reason they should not be held responsible.

The intermediaries should be responsible to stop the illegal activity, not simply because they are the least cost avoider, but because they are getting rich off the illegal activity. There is a normative judgment here: people shouldn’t profit from theft. The blame is usually established by reference to the large volume of revenue that the intermediary is making from the illegal transactions or the cost savings involved in not stopping the transactions. At the same time, any efforts the intermediary is involved in to mitigate the illegal activity are downplayed or ignored, making it appear that the third party is willfully refusing to do his part.

The point I am making is not that these normative considerations are somehow inappropriate and that we should go back to a hard-headed cost analysis. Rather, it is that these normative judgments are an essential ingredient in determining third party liability, and that it is better to accept that fact than to purport to reduce the question to neutral cost-benefit analysis.

### 4. Summary

An economic framework, broadly construed and supplemented with suitable considerations of equity, can be a useful way to assess the need for indirect liability for intermediaries in specific cases. The elements of the framework are as follows:

**Market Failure Analysis** Are there substantial transaction costs? Can enforcement be achieved without an indirect liability rule? Can private parties work out enforcement arrangements among themselves? Can third parties effectively work with law enforcement without an indirect liability mandate?

**Cost-Benefit Analysis** Does the burden on the wronged party or on law enforcement to take enforcement steps exceed the burden on the third parties? Are the costs of enforcement efforts reasonable in light of the reduction in harm? Are there longer-term or dynamic considerations to take into account?
**Equity Analysis** Do third parties exercise such close control over the harm that they should be held responsible for its mitigation or elimination? Are they blameworthy for not taking steps against it? Is the harm particularly egregious?

*C. Application of the Framework*

There have been a growing number of calls for imposing liability on intermediaries – through legislation, court action or negligence burdens. In some cases especially in the case of payment intermediaries who do not benefit from the tradition of immunity for pure Internet actors, legislation has been passed imposing some variety of indirect liability. What are we to make of these developments in light of the experience of intermediaries and the analytical framework we have just developed?

I apply the general framework to the specific cases below, but I want to focus here on the cost–benefit issues. The previous discussion suggests that payment intermediary action in this area has been effective. Internet gambling websites have been denied access to the U.S. market, and their current and projected revenues are in decline. Online pornography, controlled substance and online tobacco sites have been substantially eliminated from the traditional payment systems and the ongoing monitoring and enforcement actions in these areas are continuing to keep their presence in traditional payment networks at a minimal level. The result of the payment system action in the case of allofmp3 has been to confine it to its domestic market and dramatically reduce the volume of activity at its website.

So there have been measureable benefits of action in this area. However, the widespread assumption that payment system action in this area is simple and almost cost-free needs to be more carefully considered than it has been. In the discussion of payment intermediaries examples we have discovered substantial costs that should give policy makers pause before moving ahead with the imposition of an indirect liability scheme for payment providers. These include: costs of maintaining and enforcing a coding and blocking scheme, which we have noted is entirely manual and cannot be automated; costs of screening and checking the business activity of merchants entering and participating in the payment systems; costs of monitoring the use of payment systems for specific illegal activity, where we have seen that payment systems are in no better position than anyone else to monitor their systems, since any party can hire a web searching firm to look at particular activity on the Internet and there are no internal payment system indicators that can reliably replace these external monitoring efforts; costs of assessing complaints of illegality, where again the intermediary has no special expertise and indeed is often less legally experienced and factually informed that the wronged party and the allegedly bad actor; costs of defending against legal challenges to enforcement action, where as we have seen the challenge typically comes in an off shore jurisdiction and so there is no way for domestic law to prevent that legal exposure. Finally, there are longer term costs of the U.S. taking unilateral action in this area: copy cat regimes are encouraged to spring up in other areas of law in imitation of action.
already taken in some areas, and other jurisdictions think that the U.S. action has legitimated this practice and so look for ways to impose their legal regimes on U.S. actors.

The question of the reasonableness of these costs in light of the benefits achieved has not been seriously addressed. Instead, it seems to be assumed that small compliance costs are justified by large enforcement benefits. While precision in the estimates of costs and benefits is unlikely in this area, a more disciplined qualitative analysis seems required.

It is in the context of this broad framework that the question of special immunity for pure internet intermediaries must be addressed. It seems to me that exemption from liability for illegal actions in their systems for pure Internet intermediaries will not endure long if traditional intermediaries are burdened with this liability. The best argument for special treatment for pure Internet intermediaries in this area is the infant industry argument. But with the growth of pure Internet intermediaries into substantial companies this argument has less force. Going forward, the arguments will have to be developed in fact-based analyses of specific cases. As a general presumption, however, it seems to me that for both pure Internet intermediaries and more traditional intermediaries, the burden of proof is on those who want to impose liability.

It is sometimes thought that cost benefit analysis is the enemy of regulation. In principle, this is not the case. It is simply one tool for analysis. It can be turned into a procedural obstacle to regulation if a requirement for extensive analysis is imposed even in cases where the costs and benefits seem obvious. But the costs and benefits of indirect liability for intermediaries are not obvious. I hope to have shown in the previous discussion and in the discussion that follows that a careful market analysis, assessment of costs and benefits and equity analysis must be undertaken before these indirect liability regimes are imposed on payment intermediaries.

1. Internet Gambling

When looked through the lens of this framework, what lessons can we learn from the experience of financial intermediaries with Internet gambling? On equity grounds, it seems to me that the payment system connection to Internet gambling is too passive to justify the imposition of responsibility. Payment intermediaries are not to blame when others use their payment system for Internet gambling. However, many concerned about the social ills connected with gambling nevertheless want to reduce the activity, and law enforcement had come to the payment intermediaries with a request to help. U.S. financial intermediaries had already refused to sign up U.S. based Internet merchants because these merchants were not authorized to act legally in the U.S. The additional help requested from some state Attorneys General was to block offshore gambling activities and many intermediaries had done that. But these agreements did not extent to all financial institutions and did not cover all states. So a market analysis would indicate that there were still some feasible enforcement arrangements that had not been
established prior to the passage of the Internet gambling act. Finally, a cost-benefit analysis is hard to accomplish. The reduction in Internet gambling activity has been estimated, but it is harder to evaluate this reduction in economic activity. Some think of this overall reduction in gambling activity as the benefit, namely, those who view the activity itself as a social harm. Others think the only harm are the social ills associated with gambling – the under age and addictive gambling, and financial hardship that results from excessive gambling. The reduction in social ills is not easy to measure and has to be evaluated against the alternative of regulation designed to permit gambling but reduce the social ills associated with it. The intangibility of these benefits makes a full cost benefit analysis very difficult.

The case also calls for some additional observations. First, this was one of the first unilateral actions of a major jurisdiction to use intermediaries to enforce local law on the Internet. It had substantial international relations repercussions. Reactions from abroad to the U.S. Internet gambling legislation have not been favorable. Shortly after the bill was signed into law in 2006 analysts estimated that the value of British Internet gambling stocks declined by $7.6 billion. The British culture minister, noting that the industry “has been very hard hit by the U.S. ban,” and that the Internet is a “global marketplace,” urged “action at the global level.” Britain was seeking to develop a consensus on a global standard to legalize and regulate Internet gambling, and the U.S. law went in the opposite direction of unilateral action to use Internet intermediaries to close off the U.S. market.

The WTO reaction, discussed earlier, continues to create international trade and larger political issues. Among the costs of using intermediaries to bar Internet gambling transactions are international conflicts. For example, in June 2009, the EU released a report criticizing the US’s Internet gambling laws, asserting that they violated WTO agreements, and urging negotiation to resolve the issues.

Second, this example illustrates the dangers of the copycat effect, which uses the example of assigning indirect liability in one case to argue for its legitimacy in another unrelated case. The copycat effect of the Internet gambling liability rule cannot be overestimated.

Kozinski, in his Perfect 10 dissent, is a prime example of the force of the copycat argument: “Requiring defendants to abide by their own rules, which “strictly prohibit members from servicing illegal businesses,” …will hardly impair the operation of a “vibrant and competitive free market,” any more than did the recent law prohibiting the use of credit cards for Internet gambling.” As we have seen, payment system contracts bar all illegal activity, and so by this logic payment systems should be responsible for enforcing all laws everywhere. But the key point here is the effect of the Internet gambling precedent. Kozinski seems to be saying: “If it worked in the case of Internet gambling why not elsewhere?” Indeed, why not everywhere? And once the precedent is set, it is hard to return to the detailed analysis of facts to see if in a specific case indirect liability makes sense. This copycat effect is a real cost of any particular decision to impose indirect liability.
The copycat reaction could very well extend globally. In the first instance it might encourage other countries to use payment systems to implement their own Internet gambling regimes. The example, however, easily extends to other areas of law. It is worth spelling out this possibility by imagining a French court approaching the Yahoo case through its authority over French financial institutions. In the actual case, a French court attempted to put obligations directly on Yahoo, a U.S. company, to prevent the online sale of Nazi paraphernalia to French citizens, which was prohibited under French law. It is true that the ultimate French enforcement power was over assets that Yahoo had in France, and that Yahoo could have avoided this enforcement power by simply withdrawing from France. The new U.S. Internet gambling law reveals an additional strategy that could be made available to French enforcement entities, namely, to deputize French banks to prevent any transactions involving French citizens and Nazi paraphernalia. French banks are clearly subject to French law. There is no direct extraterritoriality involved. The obligation would be similar to the U.S. Internet gambling obligation: put in place reasonable policies and procedures that prevent the use of the French banking facilities for payment of transactions involving Nazi paraphernalia.

How would French financial institutions react to this obligation? They could avoid it only by dropping out of global payment networks, something they would be reluctant to do. They would have to transmit to the global payment systems of which they were a part the requirement to observe this French obligation. These payment systems probably would not use a coding and blocking scheme because the content of retail transactions is not coded in payment system transaction messages and a code for Nazi paraphernalia would be much too specific for any business needs. To implement the rule, the international global payment system would have to put a burden on all banks in their system to arrange their contracts with merchants to ensure that none of them insert transactions in the system that involve Nazi paraphernalia and a customer of a French bank. To enforce this effectively, would involve locating the Internet sites involved in these sales, perhaps through their advertisements or through independent searches of websites looking for appropriate key words or symbols. Further steps might involve doing test transactions using a card issued by a French bank, and then taking enforcement steps against merchants found to be submitting transactions for authorization in violation of this rule.

One of the costs of the U.S. Internet gambling bill is that it legitimates the unilateral use of Internet intermediaries to enforce local law, and thereby makes it more likely. Something like a worldwide Internet trade war might very well be the result of many nations mimicking the unilateralist strategy as each nation attempts to burden global intermediaries with the obligation to enforce its local law. In the short run and for a few cases, payment intermediaries can manage the burden of being the enforcer of local laws, but they cannot possibly mimic the diversity of the world’s law in their payment mechanisms. Individual laws that make an Internet trade war more likely have a long term cost that needs to be assessed. The burden on payment intermediaries cannot be dismissed as simply a burden on them alone. They will react to the extra costs by taking steps that reduce the overall growth of electronic commerce.
The way intermediaries comply with the new Internet gambling law illustrates the point that intermediaries are usually better than others at monitoring their own systems for business activity of a certain type, but not for detecting the illegality of activity on their systems. The point arises in the context of Internet gambling because the codes used by financial institutions reflect the business activity of gambling, not its status as legal or illegal. The result is that the policies and procedures adopted by payment systems to comply with the Act, and which have been accepted by the implementing regulations, over block, preventing perfectly legal activity from taking place.

In light of this difficulty, there might be more effective ways of assigning liability than the mechanism chosen. The new law creates unnecessary confusion by failing to define the term “unlawful Internet gambling.” As Barney Frank wrote to Treasury Secretary Paulson,

“The proposed regulations, like the underlying UIGEA statute, fail to define the term “unlawful Internet gambling,” leaving it to each financial institution to reconcile conflicting state and federal laws, court decisions and inconsistent Department of Justice interpretations when determining whether to process a transaction.”

He has introduced legislation to permit and regulate Internet gambling merchants. It would require the Secretary of the Treasury to license Internet gambling establishments, and would provide for immunity for financial service companies who process transactions to licensed entities. The licensing process would be the exclusive way for Internet gambling sites to operate legally. The obligations to block transactions from other, unlicensed Internet gambling merchants would remain. But there would be no requirement to block the licensed Internet gambling merchants. The lack of clarity about which merchants were legal would be resolved through the licensing process. At its best the system would rely on a list of approved gambling entities which the payment networks could check to determine whether to approve gambling transactions from particular Internet merchants.

To be effective, however, this list would ultimately have to be coordinated with other jurisdictions. Payment systems might respond to such a new regime by updating their coding and blocking system or by requiring banks in other jurisdictions to take other steps. Either system might be manageable for the U.S. and in the short run. But the long term ramifications could be very complex. For instance, websites authorized to engage in Internet gambling by the U.S. Treasury Secretary might not be authorized by other countries. France for instance has a zero tolerance approach to Internet gambling. France could seek to enforce this law by limiting the ability of French banks to accept any Internet gambling transactions. Other countries might have their own legal requirements for registering and regulating Internet gambling establishments. Britain has such a system, as does Antigua. If these countries decide to make financial intermediaries responsible for enforcing their restrictions, then the payment network systems would have to be updated to deal with their policies.
In this way, countries could seek to build on the payment systems in the hopes of using it to enforce their local rules regarding Internet gambling. But a system that works well in the short term and for a few countries could easily collapse if each country attempts to use it for this purpose.

None of this is imminent, and if all we are looking at is the short term, the new licensing regime proposed in Barney Frank’s legislation would be an improvement over the existing system. But in the longer term the only way payment systems can operate is through a reduction in the diversity of the laws to which they must accommodate themselves. This suggests that either government seek other ways of enforcing their local laws or beginning the process of harmonizing their laws. One practical way forward in the case of Internet gambling would be an international agreement that would recognize licensing arrangements in different countries as long as they satisfied certain agreed upon minimum standards.

2. Child Pornography, Controlled Substances and Online Tobacco

These cases can be considered together because they raise common issues. They involve extensive cooperation between payment systems and U.S. government agencies involved in taking enforcement actions against criminal activity on the Internet. In the child pornography and controlled substance cases, payment systems are monitoring their systems for these transactions and sharing the results with law enforcement. In the online tobacco case, they react to complaints brought to them by law enforcement. These enforcement arrangements have been worked out in the absence of any legal compulsion.

These current actions by payment systems make sense in terms of our framework of analysis. The degree of control exercised by payment intermediaries in these cases is no greater than in their provision of services to any merchant. If all that is relevant is the extent of actual control that payment intermediaries have against online purveyors of child porn and controlled substances, then payment intermediaries wouldn’t have a responsibility to act in these areas. But the degree of harm imposed by a merchant’s activity is also relevant. The public health harm created by child pornography and online tobacco sales is very high. As a result, payment systems should take some positive steps in this area to prevent the use of their systems for these purposes. System monitoring seems needed because that is the most effective way to catch these bad actors if they manage to slip into the system.

The payment networks have calibrated their responses to the degree of harm involved and the needs of law enforcement. Online tobacco sales pose less public health problems than the other cases, and law enforcement is able to efficiently investigate cases and bring them to the attention of the payment systems. System monitoring makes sense for child pornography and controlled substances where the degree of harm is higher.

The next question is whether there is any market failure that would justify translating this general responsibility into a legal requirement. In these cases, the answer appears to be no. Intermediaries are cooperating fully with the relevant government
agencies. They are taking substantial steps outlined earlier. These steps satisfy the general obligation, and so there is no need for an additional regulatory requirement.

Despite the steps that the payment card industry has taken to cooperate with law enforcement and the success of these efforts in reducing both child pornography and illegal sales of controlled substances, Congress has acted in these areas.\textsuperscript{130}

Proposed legislation mandates further efforts by intermediaries to prevent the use of their systems for child pornography.\textsuperscript{131} For financial intermediaries, the bill would impose fines and prison sentences on anyone who “knowingly conducts, or attempts or conspires to conduct, a financial transaction… knowing that such transaction will facilitate access to, or the possession of, child pornography…”\textsuperscript{132} For other intermediaries, the bill would impose fines and prison terms on any web hosting company or email provider who “knowingly engages in any conduct the provider knows or has reason to believe facilitates access to, or the possession of, child pornography.”\textsuperscript{133} The bill also imposes a two-year record keeping requirement on Internet service providers and others to help facilitate child pornography investigations.\textsuperscript{134} In light of the extensive efforts already undertaken by intermediaries in this area, it is unlikely that these requirements will produce any additional benefit.

Congress passed legislation related to online pharmacies in 2008.\textsuperscript{135} This law imposed obligations on U.S. based Internet pharmacies in regard to controlled substances and prohibits the sale of controlled substances except as specifically authorized. It appears to impose a duty on some intermediaries. They must not “knowingly or intentionally…aid or abet…” any unauthorized sale of controlled substances. The statute provides an example of such aiding or abetting as “serving as an agent, intermediary, or other entity that causes the Internet to be used to bring together a buyer and seller to engage in the (unauthorized) dispensing of a controlled substance…”\textsuperscript{136} It is not clear, that these requirements apply to payment systems.\textsuperscript{137} In any case, it is very likely that current financial intermediary processes would easily satisfy this general requirement if it applied.

As we saw in the case of Internet gambling, the exemptions from liability first developed in conjunction with Section 230 of the Communications Decency Act for pure Internet intermediaries were continued in the new online pharmacy bill. The duties imposed on third parties not to aid or abet illegal controlled substance transactions do not apply to “the provision of a telecommunications service, or of an Internet access service or Internet information location tool…or …the transmission, storage, retrieval, hosting, formatting, or translation (or any combination thereof) of a communication, without selection or alteration of the content of the communication.”\textsuperscript{138}

This exemption from liability appears justified for these parties, since they are far removed from the actual causation of the illicit transactions, their very indirect involvement is passive and they undertake take substantial efforts to control the sale of controlled substances online. Legal liability is thus not needed and would not be likely to increase their efforts. Given the similar situation occupied by payment systems, and their
substantial role in fighting these illegal activities in conjunction with law enforcement, it seems that indirect liability for them would not be justified either.

On cost grounds, however, the current arrangements could be improved. There is no particular expertise that payment systems have in monitoring their own systems for child pornography and controlled substances. The networks have outsourced their system monitoring efforts, and some efficiency could be had by combining these efforts, in coordination with appropriate law enforcement.\textsuperscript{139}

A different mechanism for improving current enforcement efforts would be a list of companies licensed to sell controlled substances on the Internet. Monitoring by payment card companies would be greatly simplified if the U.S. government maintained a list of websites, domestic and international, that are properly licensed to sell controlled substances.\textsuperscript{140} This improvement, however, would require substantial international coordination to be effective.

The online tobacco case illustrates that law enforcement can effectively use payment intermediaries to obtain results that would be very much more expensive. But there was a legal judgment that the payment intermediaries had to make in this case. Law enforcement asserted that online tobacco merchants were operating illegally. But there was a contrary point of view. Some online tobacco merchants held that the federal and state laws did not apply to them because they were members of Native American nations, with their own sovereign rules that regulated their ability to sell tobacco products. The decision by payment intermediaries to suspend payment services unless they could prove to law enforcement that they were legal effectively took law enforcement’s side in this dispute. Greater legal clarity by appropriate judicial bodies would have avoided this need for payment intermediaries to make their own independent evaluation of law enforcement claims.

3. Online Copyright Infringement

Several observations on the copyright example might have broader implications since it is a case which relates to complaints by private parties of tangible economic harm. First, the court Perfect 10 case properly rejected indirect liability for payment intermediaries. The involvement of payment networks in copyright violations is attenuated and entirely passive. On control grounds, there is simply no way to draw a line between payment network involvement in allegedly infringing transactions and their involvement in a wide range of other potentially illegal activities. If they are liable in this case, why wouldn’t they be liable for all cases of illegal activity on their payment systems? Without meaning to, the Kozinski dissent brought out this implication.\textsuperscript{141}

It is worth being clear on what indirect copyright liability for payment intermediaries might involve. Kozinski painted a clear picture of how, in his opinion, payment intermediaries might act if they were liable under copyright for infringement:
“…the cards have the authority, given to them by contract, to force the Stolen Content Websites to remove infringing images from their inventory as a condition for using defendants’ payment systems. If the merchants comply, their websites stop peddling stolen content and so infringement is stopped or limited. If they don’t comply, defendants have the right—and under copyright law the duty—to kick the pirates off their payment networks, forcing them to find other means of getting paid or go out of business. In that case, too, infringement is stopped or limited.”

He explicitly contemplated that the U.S. based payment intermediaries would take action against parties in other jurisdictions:

“Here, plaintiff alleges that many direct infringers have no physical presence in the United States. They operate from far-off jurisdictions, where lawsuits are difficult to bring and remedies impossible to enforce because the infringers can easily move their operations to servers in other remote jurisdictions.”

But the experience of payment intermediaries in this area is that things would not be that simple. Even in the case of a well-developed and researched complaint, payment intermediaries are never presented with a question of removing “infringing” material. At best, there is a well-documented assertion of infringement under the laws of a particular jurisdiction. Kozinski appears to favor a notice and take down approach, so that payment intermediaries are not responsible for illegal conduct of which they are unaware. But as Visa found in the Allofmp3.com case, they and their associated financial service partners can be liable for wrongful termination of services in those jurisdictions if they react to an allegation of infringement by “kicking the pirates off their payment networks.”

Second, there are available arrangements between payment intermediaries and copyright owners that can be used to reduce the amount of copyright infringement on the Internet. These arrangements are informal, but are growing. They rely on complaints by copyright owners, followed by investigation and action by intermediaries. They seem to strike a cost-based balance by putting the burden of discovering copyright infringement on the copyright owner and triggering action by the third party only after notification. They might involve compensation of the payment intermediaries for performing enforcement services, but if this enables copyright owners to reduce the harm of copyright infringement they might very well be prepared to pay it. If there are extra efforts that a particular copyright owner would like payment intermediaries to make that are above and beyond the standard practices, that too should be open to negotiation. There do not seem to be any transaction costs that would prevent the parties from negotiating adjustments in these arrangements over time. There appear to be no market failures that would justify not relying on these private sector enforcement arrangements.

Third, given the legal risks involved, copyright owners should be willing to indemnify payment intermediaries for legal actions that result from their taking enforcement actions against alleged infringers. The alofmp3.com case indicates that these legal risks are not hypothetical. If the copyright owner is persuaded of the legal
soundness of his case, he should be prepared to assume the risk. It might be one way to assure that only strong complaints are brought to the attention of the payment intermediary.

It might be thought that a statute could help here by providing legal immunity to payment intermediaries when they take good faith action against alleged infringers based on complaints. But U.S. law cannot provide immunity in other jurisdictions, which is where the aid of global payment intermediaries is needed.

Fourth, this case illustrates the need for greater clarity in the legal environment in which the intermediaries operate. Intermediaries cannot be in the position of creating new global law by their own interpretation of current statutes. Again the Allofmp3.com case suggests the need for even greater harmonization of local laws that intermediaries are expected to enforce. USTR attempted to step up to do this job by working with the Russian government to bring about changes in Russian law that would bring it closer to the international norm.  

This examination of the costs and benefits of indirect liability in these cases brings into focus the long-term Internet governance issues raised by the Internet exceptionalist debate. I now turn to those issues.

III. INTERNET GOVERNANCE

In this section I revisit the issues raised by the Internet exceptionalist debate and contrast several possible views. First there is the original Internet exceptionalist perspective which viewed government regulation of the Internet as infeasible and normatively less desirable than government deference to the rules developed by self-governing Internet communities. Second, there is the perspective of the “bordered” Internet which defends the idea that at least in certain cases local governments may properly and unilaterally extend their jurisdiction over Internet activities. Standard measures to resolve conflicts of law are available in this view. An expansion of the bordered Internet view is Paul Berman’s cosmopolitan pluralism which urges resolutions of conflict of law by a “cosmopolitan” framework that recognizes that people form multiple community affiliations that are not necessarily linked to physical geography. Third, since the “bordered Internet” does not scale up, it makes sense to revisit exceptionalism in a revised form to see if it can be relied on as an appropriate framework for Internet governance. I examine Brian Holland’s revised version of exceptionalism according to which the various immunities from intermediary liability established by local jurisdictions enable the development of autonomous Internet norms. Finally, I discuss the internationalist perspective, according to which local governments exercise control over specific Internet activities in a coordinated fashion.
A. Internet Exceptionalism

In February 1996, John Perry Barlow declared cyberspace to be independent of national governments, roughly on the grounds that cyberspace “does not lie within your borders” and that it “is a world that is both everywhere and nowhere, but it is not where bodies live.” Conflicts in cyberspace would be resolved not with the territorially-based “legal concepts of property, expression, identity, movement, and context,” which “do not apply,” to cyberspace because they “are all based on matter, and there is no matter here.” Rather, in cyberspace “governance will arise according to the conditions of our world, not yours.” Cyberspace “is different.”

At around the same time, legal scholars David Johnson and David Post made a similar case for Internet exceptionalism. In their view, the Internet destroys the link between geographical location and the “power of local governments to assert control over online behavior… (and)...the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena…”. The Internet destroys the power of local governments because they cannot control the flow of electrons across their physical boundaries, and if they attempted to do so determined users would just route around the barriers. Moreover, if one jurisdiction could assert control over Internet transactions they all could, resulting in the impossibility that all “Web-based activity, in this view, must be subject simultaneously to the laws of all territorial sovereigns.” The Internet destroys the legitimacy of local jurisdiction because legitimacy depends on the consent of the governed and “there is no geographically localized set of constituents with a stronger claim to regulate it than any other local group; the strongest claim to control comes from the participants themselves, and they could be anywhere.” Because “events on the Net occur everywhere but nowhere in particular…no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws.”

Behind these arguments was an appealing political vision. The ideal envisaged was that self-organizing groups of people would make the rules that applied to their conduct. These rules would not be imposed from the outside, but would be freely chosen by the active participation of the community members. The key was deliberation by free, rational agents in their communities, not imposition of rules by an arbitrary act of will by a distant sovereign. This ideal of participatory democracy was intended in part to offset the alienating effects of large-scale modern democracies, which, whatever their traditions and rationales, in practice had long failed to provide their members with the sense of community participation that alone seemed to justify the imposition of collective rules.

The way this vision would be implemented on the Internet would be through the development of autonomous communities of Internet users. These Internet communities were largely isolated from “real world” communities. Since it took special care and effort to reach out to participate in them, only those people who really wanted to participate would and the effects of activities in those communities would be limited to those who chose to participate. Given the structure of the Internet as a communications network, which moved almost all major decisions on content to the edges of the network, a diversity of law could arise in cyberspace as each community developed its own norms for regulating the conduct of its members. People would be free to participate in the
communities they wanted, but could easily avoid those they did not like. Enforcement of the community rules would be accomplished through peer pressure, reputational systems, informal dispute resolution mechanisms, and ultimately, banishment. The system as a whole would evolve through a process analogous to biological evolution, where diverse and potentially competing rule sets as embodied in different communities would vie for acceptance in a kind of free marketplace of rules.

Internet exceptionalism is thus the view that activity on the Internet should be regulated by Internet community norms, not laws of territorial jurisdictions, or globally harmonized laws.\textsuperscript{152} It is hard to avoid the sense that the political vision pre-dated the Internet, that the feasibility argument masked the underlying vision and that the arrival of the Internet simply created the possibility of implementing the vision in a way that the “real” world did not. To see this, imagine the reaction of Internet exceptionalists to the idea of a world government that would establish uniform global laws. This would eliminate the conflict of law problem. But exceptionalists are even more appalled with the idea of world government control over the Internet than with the idea of nation state control over it. This suggests that the issue is not feasibility of control, but the value of participative community decision making and diversity.

Regardless, the desirability of the vision was immediately attacked by defenders of real world authority to regulate the Internet so effectively that many believe with Goldsmith and Wu that these notions of a “self-governing cyberspace are largely discredited.”\textsuperscript{153} As they note, the key mechanisms of government control are the Internet intermediaries who provide essential services for Internet transactions and who are located in specific jurisdictions. Government action against these intermediaries “makes it hard for local users to obtain content from, or to transact with, law-evading content providers abroad. In this way, government affects Internet flows within their borders even though they originate abroad and cannot easily be stopped at the border.”\textsuperscript{154} And these efforts to bring order to the Internet through pressure on intermediaries are often legitimate because they provide “something invisible, but essential: public goods like criminal law, property rights and contract enforcement…that only government can provide.”\textsuperscript{155}

These Internet non-essentialists maintained that regulation of the Internet was both feasible and often desirable. The realm of cyber space was not, they maintained, a separate place. Rather, the Internet was simply a communications network that linked real people in one jurisdiction with real people in other jurisdictions. Spillover harm from cyber space activity was not only possible; it was frequent and unavoidable. Local law had a perfectly legitimate role in regulating these harms. There would be conflicts of law regarding activities on the Internet, but these conflicts were not different in kind from conflicts of law in other contexts and could be handled by familiar tools such as rules to assign jurisdiction, to resolve conflicts of laws, and to recognize judgments. There was no need for a self-governing realm of cyberspace, and so no place other than the “real” world to implement the political vision that motivated the early cyber libertarians.
The debate took an interesting twist through the work of Larry Lessig. A key element of the early exceptionalist framework was the idea that the Internet had a fundamental nature, which governments did not control which they could not alter, and which effectively prevented them from imposing local rules. In his influential book, *Code*, Lessig took aim at this idea. He pointed out that computer systems, software applications, and communications networks were human creations and that the choices of the architects of these systems were embodied in the code that made it possible for these systems to run. Far from being a natural object, these systems were subject to the decisions of the parties (usually non-governmental entities) that had the right and the ability to create, maintain and alter them.

The initial openness and transparency of the Internet was therefore something that could not be assumed as a fact of nature, but something that needed to be maintained against possible opponents. But unlike the early cyber libertarians, Lessig did not focus on the dangers that local governments might try to control choices by controlling code. He thought the openness of the Internet had to be maintained against the interests of non-governmental parties seeking to advance their own strategic interests. Lessig’s initial private sector targets were the network carriers who were seeking to alter the “end-to-end” design of the network in order to pursue their own strategic interests at the expense of application providers, service providers and end users who relied on the neutrality of the Internet to conduct their ordinary activities. In this way, the Internet exceptionalist debate merged with the net neutrality debate and the original defenders of exceptionalism seemed to be faced with the (to them) unattractive dilemma of using local governments to promote Internet values of openness or allowing their Internet choices to be dictated by unaccountable private entities that controlled the fundamental architecture of the Internet.

What does the experience of global payment intermediaries tell us about this debate? Most of the initially important points have already been made in the earlier discussion. First, Goldsmith’s prediction that intermediaries can be used to effectively control activity in cyber space has been confirmed. If the idea was that government could regulate only by regulating individuals, the experience of intermediaries, as predicted by Goldsmith, is that this is wrong. “The mistake here is the belief that governments regulate only through direct sanctioning of individuals…Governments can…impose liability on intermediaries like Internet service providers or credit card companies.”

It might be thought that intermediaries can resist this imposition of local law. But they should not, at least as a general matter. They should not themselves defer to the judgments of self-governing communities of Internet users when this conflicts with local law. As corporate citizens, they have an obligation to obey the laws of the jurisdictions in which they operate, and they simply have no basis to excuse themselves from that duty in order to let online communities determine their own fate.

Second, Lessig’s points on coding are also confirmed: “coding” decisions by intermediaries can dramatically affect the ability of Internet users to engage in online
activities, and that these coding decisions, though largely at the discretion of the intermediary, can be dictated by government regulations.

The initial difficulties presented by this approach are so significant that they make it worthwhile to consider the merits of the major alternative: Wu and Goldsmith’s bordered Internet.

**B. The Bordered Internet**

Wu and Goldsmith developed a conception of government regulation of the Internet by local territorial governments which they call the bordered Internet. It seems to them to be a tolerable, desirable, and in any case an inevitable state of affairs. In contrast to the cyber libertarians, they accepted and even advocated government role in regulating the Internet. In contrast to what they called the internationalists, they wanted the Internet to stay bordered, rather than develop universal norms that would end the kind of national diversity that they found desirable. They agreed, in effect, with the libertarians that diversity was a desirable goal; they just located this diversity at the level of national governments rather than in autonomous communities of Internet users.

This world of a bordered Internet would work pretty much as the world worked before the Internet. New regulations would be crafted to deal with the new dangers specifically created by the Internet, but there would be no fundamental needed to adjust the basic domestic or international framework.

One of the major problems of the bordered Internet would be to resolve jurisdictional disputes. The initial Internet exceptionalist argument was that Internet activity was simultaneously present in multiple overlapping and inconsistent jurisdictions, and that no one jurisdiction has a better claim to regulate its activity than any other jurisdiction. It would be better to think of the activity as taking place in a separate jurisdiction altogether and have the territorial governments of the world defer to the community norms created there. The response was that Internet activity was real world activity, taking place in particular jurisdictions and that local governments could exert control over this activity by attaching obligations to the local operations of global Internet intermediaries who were subject to the jurisdiction of these local authorities. This indirect liability for intermediaries would make it easier to extend local law to the bad actor. Conflict of laws would be handled by the normal mechanisms for resolutions of these disputes, and enforced, ultimately, by actions taken against local operations of global intermediaries.

Jurisdiction in cyberspace is a complex topic with many different approaches to assigning both the applicable law and the court of jurisdiction. Standards include determining the location of the transaction and the jurisdiction and interests of the parties. An early attempt to deal with these issues in the Internet context was the Federal Trade Commission’s approach to consumer protection in the global marketplace. Transnational concerns are implicated in the simplest cross border electronic transaction. When a merchant is in one jurisdiction and the customer is in another, whose law applies? If there is a problem, where do parties seek redress? The
FTC considered arguments for the “country of origin” approach and the “country of destination” approach. Under the country of origin approach, the law of the merchant would apply and the courts of the merchant’s country would adjudicate any disputes. Under the country of destination approach, the law of the consumer would apply and the courts of the consumer’s country would adjudicate disputes. 162

The defense of the country of origin approach relied on the difficulty of applying any other legal framework to the electronic marketplace. Only this country of origin framework seemed to allow for the growth of global e-commerce. How is a small or medium sized business to keep up with the laws of 180 countries to which he might sell? And if the test is some variety of “purposeful” targeting, how could such a standard be applied? Better to provide for uniformity and predictability by creating a default rule of the country of origin.

This approach has defects. First, it would force consumers to rely on unfamiliar consumer protections. If merchants cannot be expected to know the laws of 180 countries, neither can consumers. Second, it would create a “race to the bottom,” whereby unscrupulous merchants would simply locate in a country with weak consumer protections. Third, consumers cannot reasonably be expected to travel to the country of origin to obtain redress. Fourth, consumers could not rely on their own consumer protection agencies for redress either, since these agencies would also be unable to enforce the consumer’s home jurisdiction protections.

So neither default rule seemed to be the right answer. As a practical matter, consumer education, self-regulatory efforts and the development of codes of conduct by multinational organizations were the means chosen to address the cross–border consumer protection issue.163 For the rest, the traditional tools of international conflict of law resolution would have to suffice.164

Some commentators such as Paul Berman attempted to reach beyond the traditional dispute resolution mechanisms for resolving conflict of law cases with principles that took into account the realities of multiple community affiliation. This was necessary in party because of the complexities created by the expansion of interconnections and multiple community affiliations made possible by the Internet. His “cosmopolitan pluralism” was “cosmopolitan” because it went beyond the laws of any one particular jurisdiction and recognized the legitimacy of norms created by private parties and communities. It was plural because it did not dissolve the multiplicity of community affiliations and their associated norms into a single world wide standard. Diversity, and conflict, would endure and would need to be resolved. The principles recommended were:

First, courts can consider the multiple domestic norms of nation-states affected by the dispute. In considering which national norms to give greatest salience, courts must consider the community affiliations of the parties and the effect of various rules on the polities of the affected states. Moreover, whereas most traditional choice-of-law regimes require a choice of one national norm, a cosmopolitan approach permits judges to develop a hybrid rule that may not correspond to any
particular national regime. Second, international treaties, agreements, or other statements of evolving international or transnational norms may provide relevant guidance. Third, courts should consider community affiliations that are not associated with nation-states, such as industry standards, norms of behavior promulgated by non-governmental organizations, community custom, and rules associated with particular activities, such as Internet usage. Fourth, courts should take into account traditional conflicts principles. For example, a useful choice-of-law framework should not develop rules that encourage a regulatory “race to the bottom” by making it easy to evade legal regimes.\textsuperscript{165}

In applying this approach to the Yahoo case, Berman notes that a court should take into account that Yahoo appeared to put itself under French jurisdiction through a series of measures aimed at the French population, including targeting ads in French to visitors to its U.S. site who appeared to come from France, and that this argued for an application of French law to its activities.

These approaches to resolving jurisdictional disputes in cyberspace have various advantages and disadvantages. However, payment system intermediaries needed a mechanism to address the jurisdictional question as they approached the question of how to take action against illegal transactions in their own system that was easy to apply, effective in resolving the dispute and minimized legal risk to the system or its members. It could not wait for unpredictable, after the fact judgments by courts. The idea they developed was that a transaction is unacceptable in the payment system if it is illegal in the jurisdiction of either the buyer or the seller.\textsuperscript{166}

What does this payment card approach contribute to this discussion? It provides a simple default rule for intermediaries to apply when determining whether to allow transactions in their systems. No one has to go through the heavily fact-based balancing assessments to determine on a case by case basis whose law applies. Nor does it simply adopt a country of origin or country of destination perspective, each of which is limited. It does not leave the transaction in a legal limbo either, where no law applies.\textsuperscript{167}

The payment system experience leads to several observations. First, direct conflicts of law are not as frequent as some thought they would be. Technology and payment system practices effectively reduce these conflicts to the rare instance where the law of one country demands what the law of another country forbids. Directly contradicting laws are more common in “political” areas, where governments are seeking information from intermediaries to enforce local laws against its own citizens.\textsuperscript{168}

Second, the method chosen to regulate the Internet of focusing on the local affiliates of global payment operations does not require the use of either the traditional or the new “cosmopolitan” conflict resolution methods. By relying on global payment intermediaries, local jurisdictions reach out to the local affiliates that are totally within their jurisdiction. They do not put burdens on entities in foreign jurisdictions at all. There is literally no conflict and so nothing for the normal mechanisms of conflict resolution to attach to.\textsuperscript{169}
The adoption of this rule by global payment intermediaries reduces the strength of the Internet exceptionalist argument about multiple jurisdictions. By concentrating enforcement in intermediaries, not on individuals or merchants, local jurisdictions can take advantage of the economies that these institutions make possible.

Holland has objected to thinking of Internet transactions as subject to multiple jurisdictions as follows:

Thus, where the Internet is understood as an undifferentiated and pervasive environment in which actions are simultaneously subject to innumerable territorially-based legal regimes, it is the perceived threat of arbitrary power - that which inherently arises from primary rules of obligation that are uncoordinated, duplicitous, contradictory, inadequately publicized, as a practical matter unstable and inconsistent, and in practice impossible to follow - that poses the greatest threat to individual autonomy and human dignity. For instance, imagine that you were able to gather a comprehensive list of all of the laws of all the countries in which the Internet is available, and that you were somehow able to cross-reference these laws such that you were able to identify all laws that would apply to a particular act. Assuming the principle that people should be ruled by the law and obey it, if any of those laws prohibit the particular activity (regardless of the legal regime from which the law originates), then you should not engage in the activity - even if the vast majority of legal regimes permit the act. But what if one legal regime requires a certain act, while another prohibits it? Your only choice is to avoid the Internet altogether, eliminating your exposure to multiple legal regimes. 170

The intuition here is correct. The extent of overlapping and inconsistent jurisdictions does limit the ability of these jurisdictions to unilaterally regulate the Internet. But the location of the difficulty is misidentified. For example, the argument seems to hold that if a person in Russia sends a copyrighted work to a person in the United States, and the transaction would be legal if conducted solely within Russia, and illegal if conducted solely within the United States, then either the transaction must be allowed everywhere if Russian law applies or blocked everywhere if U.S. law applies.

The mistake is to ignore the technical ability of global payment systems to reduce transactions to events in which only a buyer in one jurisdiction and a seller in another are implicated. In the above example, the transaction is illegal for buyer, and so cannot be allowed. But a similar transaction conducted solely within Russia would be legal and could be permitted by the payment system. If the United States makes Internet gambling illegal for U.S. citizens, Internet gambling merchants do not need to abandon the Internet. They do need to code their transactions properly in payment systems, and then rely on the coding and blocking mechanisms governing these systems to ensure that the transactions are permitted where legal and blocked where illegal.
The experience of payment intermediaries is that within limits the differences among conflicting jurisdictions can be managed. The bordered Internet seems to work as long as the scale is small. So far, the scale is small for two reasons: the number of cases of governments reaching across borders to inflict their laws on Internet merchants in other jurisdictions is still relatively small. The U.S. Internet gambling law is the most salient. Moreover, in contrast to the rhetoric about the Internet creating a global marketplace, the scale of cross-border commerce itself is still small. The reality is the volume of cross-border transactions is not large enough right now to create a truly substantial cross-border jurisdictional crisis.

Cross-border commercial transactions actually represent a small volume of all Internet traffic. In the US, only 4% of the sales for electronic commerce merchants come from abroad.\(^{171}\) And data from Europe show that cross border transactions are not increasing as fast as overall ecommerce transactions:

> While e-commerce is taking off at national level (in some countries), it is still relatively uncommon for consumers to use the Internet to purchase goods or services in another Member State. As a result, the gap between domestic and cross-border e-commerce is widening: from 2006 to 2008, the share of all EU consumers that have bought at least one item over the Internet increased from 27% to 33% while cross border e-commerce remained stable (6% to 7%).\(^{172}\)

Electronic commerce is growing. But cross-border electronic commerce is not. Even when they use the Internet, people still want to buy locally, not globally. As long as cross-border transactions remain a relatively small portion of the overall total of transactions, the problems created by overlapping and inconsistent regimes will likely remain small.

The fourth point is a reiteration of David Post’s warning: things might be ok now, but just wait. The problem the Internet creates for local jurisdictions is one of scale.\(^{173}\) The system simply does not scale up. As we have seen global payment systems cannot accommodate an enforcement burden in which each jurisdiction uses payment system mechanisms to enforce each of its local laws on the Internet. And the chances of the rest of the world engaging in copycat regulation of the Internet based on the US example are reasonably high.

It is not hard to see how we can get into a kind of tragedy of the commons in this area. Each individual extension of local jurisdiction into cyber space seems small and costless, but collectively the burden becomes unbearable. Governments might feel free to exploit this enforcement mechanism, in the same way that grazers use the commons – under the impression that it is an unlimited resource. But as the cross-border rules pile up, one of two things will happen: either cross border transactions will remain small and the potential for the Internet to be a global channel of commerce will not be realized or the political costs of each government attempting to regulate the ecommerce activities of other countries will mount up. Either development reveals the limitations of the bordered Internet as a long term framework for Internet governance.
Goldsmith and Wu suggest that the enforcement of Internet regulations through intermediaries is necessarily limited in size. Maybe the system won’t be able to scale up, they seem to be saying, but it won’t have to. Small countries such as Antigua cannot enforce Internet rules because global intermediaries can simply pull up stakes and leave if the rules are too strict. But there are a sufficiently large number of countries that global intermediaries do not feel capable of abandoning so that the system can be overwhelmed if all of them use the intermediary enforcement mechanism.

Intermediaries can mediate some of the conflicts of jurisdiction raised by the early Internet exceptionalists. A single payment system can reach the thousands of Internet sites and consumers engaged in illegal actions and efficiently bring these entities under local jurisdiction. But this centralization function has natural limits. At some point, the same problems of conflicting and overlapping multiple jurisdictions will overwhelm the ability of these payment systems to manage the conflict.

These long term difficulties of the bordered Internet suggest that we give exceptionalism another look.

C. Exceptionalism Revisited

Proponents of a revised Internet exceptionalism start from the premise that the ideal of self-governing autonomous Internet communities is still valid. This ideal is exactly what was lost in the Lessig debate over code and architecture. One version of the revived exceptionalism defended by Brian Holland focuses on Web 2.0 communities, and argues that together with the immunity provisions of Section 230 of Communications Decency Act, these communities have the potential to allow the growth of internal community norms to take the place of external territorially-based laws. This turns into a defense of Section 230: policy makers should preserve this immunity because it allows Web 2.0 communities to implement the kind of desirable self-governing structure that the original visionaries had in mind. While it is feasible to repeal this immunity, and impose indirect liability on Internet intermediaries, this way of enforcing local territorially based laws is normatively undesirable and should be resisted.

In addition to promoting this desirable form of self-government, this perspective could rescue us from the scale problems of the bordered Internet. If governments voluntarily resisted the call to use intermediaries to regulate the Internet to the greatest extent possible, then the burdens on intermediaries would remain small and manageable.

Holland does not re-fight the sovereignty battle. He emphasizes that his modified version of exceptionalism was created and is maintained by local sovereign law. He also notes many of its limitations. It is bounded by contract law, criminal law and intellectual property law, and is widely not shared by other local jurisdictions outside the United States. But his strongest point is that the new Web 2.0 communities will in fact
take advantage of this immunity to allow self-governance. His examples include social networks such as Facebook and wiki sites such as Wikipedia. 

I do not dispute the conclusion that pure Internet intermediaries should continue to be exempt from indirect liability under Section 230. The connection between the passive actions of the Internet intermediaries and the aggrieved party harms is too attenuated to assign responsibility. To the extent that these intermediaries can reasonably take steps to prevent the users of their systems from causing harms to other parties they have already put in place extensive policies to do so. So it is not clear that further indirect liability will result in benefits that are commensurate with the additional enforcement costs.

But I am skeptical of the Internet exceptionalist rationale for this conclusion. It paints the Internet intermediaries in an overly optimistic light. The key objection is this: the “law” of Internet communities is not really the law of that community. It is a commercial contract enforceable under the rules of some local jurisdiction or other and the terms of the contract are and should be subject to the same kinds of legal and regulatory oversight that bind contracts between people in local jurisdictions. For this and other reasons, it seems highly unlikely to me that Web 2.0 communities really will develop the kind of self-governing structure that Holland envisages.

The first thing to not about the section 230 immunity is that it is extremely limited, even more so than Holland notes. Second, it is extremely unlikely that the Web 2.0 companies will in fact allow the kind of self-government that Holland imagines. Third, additional regulations are needed to fully protect members of these communities. I focus on competition policy, privacy and consumer protection as examples. Fourth, legal discretion granted to intermediaries today is too broad and should be limited by replacing intermediary judgment with public authority decisions.

1. Scope Limitations

Section 230 doesn’t suspend the laws of local jurisdictions. It does not prevent the application of U.S. law to the pure U.S. Internet intermediaries. Antitrust, privacy laws and consumer protection laws, among all the others, continue to apply. It simply says that pure U.S. Internet intermediaries are not themselves liable for certain actions of people who use their system. These actions by others continue to be illegal under US law. The ISP or web hosting service might not be liable for a user’s posting of a defamatory note on a bulletin board under 230, but a U.S. citizen who posted it would be liable under regular U.S. defamation law and if he were identified he could be prosecuted. If an online community suggested, that in contravention of French law, they intended to allow unrestricted trafficking in Nazi paraphernalia in their community, French citizens would still be in violation of French law if they obtaining these prohibited items from that online community.

Furthermore, intermediary enforcement is still possible despite Section 230. It does not apply to all intermediaries. It does not apply to U.S. payment intermediaries,
who could be required to block transactions involving payments for illegal content. It does not apply to French ISPs, or to French banks. France could still order its local banks not to facilitate payment for membership by a French citizen in an online community that allows transactions involving Nazi paraphernalia.

So the continuation of Section 230 Internet immunity is perhaps necessary for the development of internal communal norms, but it doesn’t really “allow” it, or at least not very much of it.

2. Likelihood of Community Control

Even if some mechanism could be developed to exclude a substantial portion of external legal norms and thereby allow for the development of internal norms, that still does not imply that the internal norms will emerge from the desirable process of debate and deliberation that Holland envisages. As Holland notes, “external legal norms are excluded, but internal communal norms are often unable to coalesce to take their place” because enforcement is “concentrated in private commercial entities.”

The modified Internet exceptionalism hope is that the intermediaries who control the new Web 2.0 platforms will be driven by internal incentives to accommodate the wishes of the online communities they create. These internal incentives include: “the need for financial support from community donations, a communal desire for information integrity, or the need to build an audience for advertising.”

But it is not clear that Web 2.0 platforms are very likely to grant this kind of democratic self-governance. For one thing, intermediaries can be subject to pressure. Craig Newmark, the operator of Craigslist, has insisted that he made his decision to remove ads for erotic services as a result of consultation with his online community. But it is also true that Craigslist was under criminal investigation by a number of state Attorneys General for violation of state laws against prostitution. One could argue immunity in this case, but Craigslist did not. It complied with a law enforcement request to remove certain postings and this decision to remove these ads will be subject to ongoing oversight by these law enforcement agencies.

If the Craigslist community voted to keep these ads in place, would Craigslist take the legal risk involved?

In addition, Web 2.0 platforms are largely commercial ventures that often respond to normal business motives. From the point of view of these commercial operators, these platforms are often less communities of like-minded individuals, and more agglomerations of customers. Indeed, many of these “communities” simply are loose collections of individuals linked by contract for relatively narrow purposes.

These communities are not governed by democratic voting procedures that guarantee the consent of the government. They are private entities, normally set up for commercial purposes and can hardly be expected to be run by someone other than their management and owners. They are governed by contractual terms of service. Often
prospective members of these communities have a simple take it or leave choice when they decide to join.\textsuperscript{183}

And this might be the way consumers want it. Online communities might not offer to determine their online laws through a political process because the members of the community cannot be bothered. People visit lots of different websites and use many different web services. It is hard to believe that they want full democratic participation rights to set up the rules for each of these services. And it is implausible that they would actually spend the time, if they were offered the opportunity.

The example of privacy policies makes the point. A recent study concluded that if all U.S. consumers read all the privacy policies for all the web sites they visited just once a year, the total amount of time spent on just reading the policies would be 53.8 billion hours per year and the cost to the economy of the time spent doing this would be $781 billion per year.\textsuperscript{184} Do people want to devote even more time to the construction of individual policies for each of the sites they visit?

Market logic is often used at this point to transform consumer sovereignty into community control. If a platform operator doesn’t respect the wishes of the community he creates, then the community will go elsewhere. This has an appeal to it – instead of fighting with a network operator who defines his interests too narrowly and fails to respect the community, community members will just use their exit rights and go to an operator who will so respond. This is not the exercise of democratic self-governance, but it might force operators to provide a framework that allows it.

The problem here is the underlying economics of these platforms don’t always allow for full consumer choice. Network effects in these markets mean that people want to be on crowded platforms, in large, not small communities. Scale economies mean that it is cheaper per community member to maintain the infrastructure necessary for the platform to function when the community is large. The consequences of these twin economic forces are that there will be few platform providers in any community category. Facebook and MySpace are the two dominant providers of social networks. There is only one substantial online peer produced encyclopedia, Wikipedia. YouTube is where everyone wants to put their videos, and eBay is by far the largest online market.\textsuperscript{185}

The limitation on consumer choice in this area restricts the ability of community members to control the platform provider by leaving. This leaves protest. This can be effective, as it was in the recent case of users objecting to the change in terms of service unilaterally offered by Facebook. By threatening the privacy rights of the community, the platform had stirred up substantial community unrest and ultimately the new terms of service were withdrawn.\textsuperscript{186}

As part of this reaction, Facebook took some steps in the direction of community self-governance. In February 2009, it proposed new privacy rules according to which users will own and control their own information, and in April it allowed a vote of its
users on these new principles. Over 75% of those voting endorse them, and on July 1, 2009 it adopted them.\textsuperscript{187}

But there are limits to protest. What if Facebook had not responded to community objections? Would people actually have left? Where would they have gone? Lock-in is a real restriction in social networks. Privacy advocates had anticipated this by threatening to file a complaint with the Federal Trade Commission at the same time as they helped to organize community objections. Privacy decisions by social networks are also subject to local law and are not simply up to the terms of service offered by platform operators.\textsuperscript{188}

3. Regulations

The exemption from liability based on Section 230 does not mean that online entities are exempt from local law. But there are three areas where regulation of online communities by governments seems especially timely and urgent - competition policy, privacy and consumer protection.

Concentration in particular sectors of the online world needs to be examined because it can so significantly reduce consumer choice. The Department of Justice has indicated, for example, that it is going to take a more active approach in this area.\textsuperscript{189} They and the Federal Trade Commission have initiated inquiries focused on the search engine market.\textsuperscript{190}

Privacy and security rules need to be defined as well. The Federal Trade Commission has taken major action in this area\textsuperscript{191} and is stepping up their enforcement. They are also clearly focusing on the development of a new privacy framework to analyze the basis for the harms associated with privacy violations.\textsuperscript{192} They have also focused on the development of rules for online behavioral advertising.\textsuperscript{193} In addition, rules governing privacy for online cloud computing services need to be clarified, perhaps by additional legislation to clarify the current framework.\textsuperscript{194}

Consumer protection rules need to be updated to apply more effectively to new developments in electronic commerce including mobile commerce, the greater availability of digital goods online, user-generated content online, the development of consumers as online sellers and new developments in accountability and payment protection. A timely development might be the harmonization of consumer redress and liability rights across various payment mechanisms.\textsuperscript{195}

4. Intermediary Discretion

The discretion of Internet intermediaries over which transactions to allow must be subject to public scrutiny. Intermediaries exercise judgment today over which transactions are subject to such legal risk that they cannot be allowed. These decisions are made in the context of the business interests and technological capabilities of the
intermediaries themselves, but they have important effects on the rights and interests of other parties. Some examples from the previous discussions include:

- Payment systems effectively decide which Internet gambling transactions are illegal. By choosing to block all coded gambling transactions, the system disadvantages horseracing, state lottery and Indian gaming transactions that are arguably legal.

- Payment systems take complaints from third parties and make an independent legal assessment of the merits of the case and withdraw service based on these assessments. Effectively, they adjudicate these copyright cases.

- Payment systems looked at the legal arguments from state AGs and BATF and determined that they were stronger than the arguments of the online tobacco merchants.

- Payment systems chose to adopt lists of dangerous substances from the FDA and DEA lists and determine that they cannot be sold by Internet pharmacies.

These decisions seem sound and sensible ways of balancing complex and competing interests. But they were private sector judgments, inevitably subjective and influenced by the particular interests of the parties involved.

Other intermediaries also have enforcement abilities that they can use at their own discretion. For instance, in June 2009, it was reported that a British ISP had agreed to disconnect subscribers who were accused of infringement three times by a copyright owner. Allegations of violations would be made by a contractor working for the content owner and transmitted to the ISP. Other enforcement efforts in that arena are under consideration, including the use of deep packet inspection of Internet traffic to detect illegal transmissions of copyrighted material.

At this point, these decisions are largely up to the payment intermediaries and ISPs themselves. They are not dictated by government requirements. Yet their decisions will have profound effects on the shape and direction of electronic commerce. Deferring to the norms of the Internet community in this context means deferring to these private judgments of intermediaries.

To the greatest extent possible, the legal system should minimize these subjective decisions by intermediaries and replace them with public decisions by responsible government bodies. But for this to happen we have to move away from the vision that says autonomous communities of Internet users should be able to make their own decisions.

I do think there is a role for Internet community decision making. The best circumstances for deference to law constructed for and by particular Internet communities is when an Internet community’s norms do not “fundamentally impinge
upon the vital interests of others who never visit this new space.”197 This sound like a version of the principle for deciding when a national law should pre-empt more local laws: if the local law doesn’t significantly affect the lives of those living in other jurisdictions, then why should the law of the larger communities prevail? To the extent an Internet community is self-contain or its activities affect others only on a voluntary basis, then there is a case for deferring.198

Internet exceptionalists are wrong to think that this deference is always or even usually the right policy. They are right, however, about a fundamental point: that the Internet creates such a potentially large number of jurisdictional conflicts that the application of the traditional ways of resolving these difficulties won’t work in a timely and predictable fashion. Global payment intermediaries will not wait for these resolutions, since they want to do business everywhere. They will instead attempt to adapt their systems to the rules of the jurisdictions they are operating in: if a transaction is illegal in a particular jurisdiction, they will attempt to eliminate from their systems. We know where that road leads, however, and we do not want to go there.

D. Internationalism

We are back to the bordered Internet where “nations have a right and a duty to protect their citizens from harm, whatever the source and whatever the medium”199 and the basic question is whether the Internet “should be regulated globally or locally.”200 The fundamentally correct insight of the Internet exceptionalists is that the unilateral imposition one nation’s law onto all Internet activities that cross borders is ultimately infeasible. It won’t scale.201

Internationalism might be the way out. It is the idea that the Internet will eventually be governed, at least for some services, by global institutions and arrangements and that this is the right public policy for local governments to follow in their dealings with illegal cross border Internet transactions. This policy could be implemented through a uniform global standard, or any of a variety of techniques such as WTO rules that bring local laws into harmony or allow them to interoperate. The basic justification for this policy in a particular case is similar to the justification for establishing a single uniform national policy that prevents the clash of inconsistent policies at the state or local level: when activities have widespread and significant effects on those outside the local jurisdiction, then uniform principles or some other coordinating mechanism should be adopted at the higher level.

Goldsmith and Wu describe the internationalist strategy. “If the nations of the world can agree to a single global law for questions like libel, pornography, copyright, consumer protection, and the like, the lives of Internet users become much simpler: no conflicting laws, no worries about complying with 175 different legal systems, no race to the bottom.”202 This would also benefit nations: “Rather than suffer through the mutually destructive effects of unilateral attempts to govern the Net, nations should come up with a
compromise global solution that would make all or most nations better off by halting the Net’s most destructive effects.” Universalism also promises better laws: “International standards could reflect a kind of collection of best practices from around the world – the opposite of the tyranny of the unreasonable.” They comment that the WTO case “seems to fulfill the Internationalist prediction that the Internet would ultimately be governed by global institutions and global laws.”

Goldsmith and Wu criticize the development of global law by comparing it unfavorably to a bordered Internet subject to conflicting local laws. First, a system of universal laws would be unattractive; it would leave the world divided and discontented because the universal law would be unpopular in large segments of the world population. Second, the system of local national laws would better reflect differences among people. Diversity is a good thing and cannot be taken into account by a universal code that overrides local differences. Third, it is not needed. The conflicts of laws, extraterritoriality and so on are perfectly manageable within the current international framework. For example, since most Internet users do not have assets in other countries, they are effectively subject only to the laws of the country where they live. Only large multinational companies with assets all over the world face the multijurisdictional problem, and they already have to live with that because they are already global. Compliance with a plurality of international laws is simply a cost of doing business for global companies. There’s nothing new here that would justify a move to a more harmonized global order. There are extra costs to be sure, but nothing so onerous or burdensome that it would require a move to global law.

The responses to these criticisms are straightforward. An unpopular global law is not the goal. Nor is the suppression of diversity the goal. The idea is to integrate local laws in some fashion when the regular conflicts among them prove to be intolerable. When diversity does not create this difficulty, there is no need for integration. If, for example, local governments value diversity enough to refrain from using intermediaries to enforce local laws against actors in other jurisdictions, then there is no need for harmonization of these enforcement efforts. But to the extent that governments want to take global enforcement steps, they need also to take steps to integrate the laws they want to enforce. And the reason for this is that the costs on global intermediaries of trying to mediate the conflicts associated with unilateral attempts at local regulation of the Internet will be so onerous and burdensome that they will cause an unwarranted and unnecessary decline in global interaction.

Berman also describes how the internationalist hope of global standards avoids the conflict of law problem: “…if we constructed one universal “world community” with one set of governing rules, there would never need to be a “choice of law” in the sense that conflict-of-laws scholars use the term.” He is critical, however, of this universal world community:

First, it tends to require that we see ourselves primarily as citizens of the world and therefore tends to dissolve the multirootedness of community affiliation into one global community. Second, it fails to capture the extreme emotional ties
people still feel to distinct transnational or local communities. Thus, universalism may ignore the very attachments people hold most deeply. Third, as Anupam Chander has pointed out, the aspiration that we become solely citizens of the world is at least partly based on an internationalization of John Rawls’s theory of justice and is therefore subject to the same criticism Rawls has long faced: that his theory assumes a self detached from the social and cultural context that makes such a self possible. Fourth, an ongoing system of universal governing norms poses such a strong challenge to our current notions of nation-state sovereignty that, as a practical matter, it seems unlikely to be adopted widely in the foreseeable future. Fifth, and perhaps most importantly, in order to create a set of universal legal norms that overrides local variation, one needs to presuppose a world citizenry devoid of both particularist ties and normative discussion about the relative importance of such ties. Thus, universalism can cut off debate about the nature of overlapping communities just as surely as territorialism or parochialism does.  

These objections can be met at the level of generality at which they are cast. We do not need to think of ourselves as primarily world citizens in order to endorse specific global approaches. We can still have deep attachments to local communities and can still debate the relative importance to us of the overlapping communities we participate in. The global approach endorses the view that self-government requires “a politics that plays itself out in a multiplicity of settings from neighborhoods to nations to the world as a whole…” and “citizens who can abide the ambiguity associated with divided sovereignty, who can think and act as multiply situated selves.” But participation in global community and the wisdom to know when the global perspective needs to take precedence over more local concerns is essential to this vision of self-government in a global world.

The internationalist proposal is to provide global coordination only when necessary. It is to move to global standards when, as a practical matter, the burdens of allowing diverse local rules are too high. The model of national uniform standards is appropriate: not everything has to be done at the national level, but some things should be done there in order to have an efficient and fair national system. In a similar way, we don’t need to move from the current system to a world government. But if there are practical ways to improve Internet governance through global harmonization they should be taken.

I do not endorse the use of intermediaries to enforce local law without the extensive analysis discussed in Section 2. But there might be arrangements, from the perspective of global coordination, which could improve the use of intermediaries as enforcers of local law. For example:

- In the Internet gambling context, a move to an internationally interoperable licensing system that would have each jurisdiction that allows Internet gambling to defer to the licensing decisions of other jurisdictions
• In the controlled substance and child pornography context, a globally coordinated web searching mechanism that would replace the individual monitoring efforts of the intermediaries.

• In the controlled substance context, an intentionally accepted list of controlled substances and entities licensed to provide for sale online.

• In the copyright context, the continued evolution of uniform copyright rules.

International agreements are one mechanism to create coordinated action. Although controversial because of the secrecy involved in its development, and the sense that affected parties were excluded from participation, the Anti-Counterfeiting Trade Agreement (ACTA) is a reasonable though flawed model for action in this area.\textsuperscript{211} The notion behind the trade agreement is that governments would agree on common enforcement measures to make sure that trade in counterfeit merchandise met uniform and coordinated government responses.

The mechanisms of international coordination are many. The OECD and APEC are multinational institutions devoted to the development of global standards in large areas of public policy and the World Trade Organization has been effectively setting international standards for several decades. The decision regarding which mechanism to use to coordinate local government efforts to regulate the Internet through intermediaries depends on the issue and the fora available for resolution.

Internationalism has its dangers. Why should each jurisdiction have the same regulations on hate speech and the same regulations on alcohol consumption? The answer is that where there really are such fundamental differences there will be no harmonization, and intermediaries will be called upon to resolve the issue themselves or will be caught between warring governments and forced to choose sides. But efforts should be made to minimize such differences when these differences have global consequences, especially when they are accidental surface differences that reflect no fundamental divisions. For the same reason that we want uniform global technical standards for information and communications technologies, if possible, we want similar legal frameworks if governments are going to enforce laws on the Internet.

These efforts to ease the friction involved in extending government authority to the Internet through a global framework are in line with other efforts to create global frameworks that promote the growth of the Internet. We saw earlier the need for regulation on Internet activity in several areas. But this regulation has a global dimension. The 30th International Conference of Data Protection and Privacy Commissioners adopted a resolution to create a working group to draft international standard on privacy. This draft standard is to be submitted to the 31\textsuperscript{st} International Conference in Madrid in November 2009.\textsuperscript{212} There is also likely to be a renewed push for global consumer protection on the occasion of the 10\textsuperscript{th} anniversary of the OECD’s Guidelines for Consumer Protection in the Context of Electronic Commerce.\textsuperscript{213}
Both these efforts relate to the growth of the Internet as a vibrant international marketplace. They do this by building online trust. Global information security standards reassure people that their information is safe no matter what the physical location of the websites they visit. Establishing global privacy standards means that the collection and use of online information will be governed by common principles regardless of website’s jurisdiction and will make it easier for global business to transfer information from one jurisdiction to another in a seamless manner. Finally, effective global consumer protection rules will mean that people will have the information and redress rights they need to shop confidently online no matter where the website is located.

V. CONCLUSION

The initial demand from Internet exceptionalists that the online world be left alone by governments has morphed, as we have seen in this discussion, into the demand that governments create a global framework to protect and spur the growth of the Internet. The intervening steps in this development are not hard to trace: Internet exceptionalists confused their ideal of self-governing Internet communities with Internet essentialism. Internet essentialism was undermined by the recognition that the coding that underlies Internet applications and services is a matter of choice, not unchangeable nature. If something about this system created difficulties for government control, this could be changed. The idea that government could not control the Internet was undermined by the ability of local operations of global intermediaries to provide essential services and the ability of governments to control these intermediaries. We have seen examples from the payment card world of how this was done in the case of Internet gambling, child pornography, controlled substances, online tobacco, and copyright infringement.

These examples proved that intermediaries can control the content of the activities on their online communities, and that government can compel or pressure intermediaries to take these steps. Intermediaries have a general obligation to follow the law, and so except in extreme cases, they have no right to resist these lawfully established burdens.

But should the government do this? The advantages of government intervention sometimes appear to be substantial, but nothing in the least cost arguments suggest that Internet intermediaries are always the best vehicle for government control. The costs, benefits and equities involved in specific cases have not been adequately assessed. Intermediaries are often in a position to voluntarily police their own communities and have taken steps to do this without explicit government requirements. The equities set out in current law establish a regime that works tolerably well. Even when government requirements are explicit, as in the Internet gambling case, they are often crafted to fit the architecture and structure of the intermediaries themselves. While some adjustments would improve these legal regimes, nothing suggests that more liability would be an improvement. Nor would a return to Internet exceptionalism help matters.
What would be an improvement is for greater government coordination on the rules that intermediaries must follow on the Internet. To avoid legal liability and to comply with local laws, payment intermediaries are moving toward a situation of accepting the laws of all jurisdictions. They also have wide discretion on what activities to allow on their systems. But this situation has problems. Intermediaries are not the best place to lodge the decisions on what rules to follow. No laws are self-interpreting. How they apply to particular situations is often obscure and heavily fact-dependent. This play in adjudication decisions leaves room for private, strategic and unaccountable decisions by intermediaries that affect the shape and direction of online activity. Coordinated government rules are best for an additional reason: the intermediary role does not scale well in a world of multiple, overlapping and conflicting rules. If governments are going to use intermediaries to regulate the Internet, they need to coordinate their own laws to make that role possible.

3 See, for example, Reno v. American Civil Liberties Union, 521 U.S. 844 (1997) and Center For Democracy & Technology V. Pappert Case No. 03-5051 (E.D. Pa. Sept. 10 2004).
4 See Ronald J. Mann & Seth R. Belzley, “The Promise of Internet Intermediary Liability,” 47 William and Mary Law Review 239 (2005) (Mann and Belzley)
5 See Debra Spar, Ruling the Waves, Harcourt, 2001, especially pp. 11-22 (Spar). Mann and Belzley at p. 3 and Goldsmith and Wu at p. 124 explicitly rely on her work. A more traditional framework expands the Spar’s innovation and commercialization phases into a sequence of invention, where the basic scientific discovery takes place, innovation, where it is initially applied in a commercial setting and diffusion, where it is spreads through industry and society. See Daniel Bell, The Coming of Post-Industrial Society, Basic Books, 1999, especially the Foreword for a good discussion of inventions, innovations and diffusion. See also Everett Rogers, Diffusion of Innovation, Basic Books, Free Press, 1962 for a summary of how innovations move through cultures and societies. Chapter 4 contains his famous early adapter theory.
6 See Spar Chapter 3.
7 See David G. Post’s elegant take on Internet exceptionalism in In Search of Jefferson’s Moose Oxford University Press 2009 (Jefferson’s Moose), especially Chapter 11 on governing cyberspace through law. See also his earlier “Against “Against Cyberanarchy,”” 17 Berkeley Technology Law Journal 1365 (2002) (Against Against). The heart of the response to Goldsmith is that scale matters and that while it is physically possible and permissible under current “settled” law of cross-border jurisprudence, it is not “workable” to subject all websites to perhaps hundreds of different and possibly conflicting jurisdictions. See Against Against p. 1384
8 See Brian Holland, “In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism,” 56 Kansas Law Review 101 (2007) (Holland). Holland’s version of modified exceptionalism is closely connected with the legal principle that online intermediaries are not liable for third party conduct. See p. 129 where he asserts that the immunity from liability created by Section 230 of the Communications Decency Act “helps to effectuate a modified form of exceptionalism by moderating the imposition of external legal norms so as to permit a limited range of choices—bounded, at least, by criminal law, intellectual property law and contract law—in which the online community is free to create its own norms and rules of conduct.”
9 See 47 U.S.C. §230(c). This immunity does not extend to criminal law contract law, or intellectual property law.
Participants in Google’s advertising programs “shall not and shall not authorize any party to…advertise anything illegal or engage in any illegal or fraudulent business practice.” See Google Inc. Advertising Program Terms at https://adwords.google.com/select/tsandcsfinder. MasterCard has rules for both merchants and their acquiring banks: “A Merchant must not submit for payment into interchange, and an Acquirer must not accept from a Merchant for submission into interchange, any Transaction that is illegal.” See MasterCard Rules at 5.9.7 at http://www.merchantcouncil.org/merchant-account/downloads/mastercard/MasterCard_Rules_5.08.pdf. For their issuing banks, they require that: “A Payment Transaction may not be effected for …for any illegal purpose.” See MasterCard Rules at 5.9.7 at http://www.merchantcouncil.org/merchant-account/downloads/mastercard/MasterCard_Rules_5.08.pdf. Visa has similar rules. For example: “A Merchant Agreement must specify that a Merchant must not knowingly submit, and an Acquirer must not knowingly accept from a Merchant, for submission into the Visa payment system, any Transaction that is illegal or that the Merchant should have known was illegal. See Visa International Operating Regulations at 4.1.B.1.c. Acquirer Penalties for Merchants Engaging in Illegal Cross-Border Transaction Activity are set out at 1.6.D.16 of the Visa International Operating Regulations. See the Visa rules at http://usa.visa.com/download/merchants/visa-international-operating-regulations.pdf.

See Holland p. 109: “Exceptionalism became an objective to be pursued and protected as a matter of choice, rather than a natural state.”

Both Visa and MasterCard evolved from an earlier association organizational structure to independent public companies. MasterCard made this transition in 2006; Visa Inc. in 2008. Visa Europe, however, retains its status as an association of European banks and is an independent entity that is the exclusive licensee of Visa trademarks and technology in the European region.

The unitary payment systems, American Express and Discover, have a similar transaction flow, but the Acquirer and the Issuer in that case are the same entity.

Internet service providers are often part of companies that also provide wireline or wireless telephone service or video programming. But in so far as they are providing Internet access they are intrinsically linked to the Internet as an essential part of their business.

They are similar to the delivery services such as UPS or Fed Ex in this respect. They provide a service that is essential to the proper functioning of electronic commerce, but are not themselves intrinsically tied to that channel of commerce.

Goldsmith and Wu discuss this example at p. 82. Mann and Belzley discuss these early law enforcement efforts at pp. 37-38.

The Wire Act (18 U.S.C. § 1084) is the federal statute used to prosecute Internet gambling activities across state lines. The way these issues were perceived in 2002 when was moving forward with Internet gambling legislation is laid out in General Accounting Office, Internet Gambling, An Overview of the Issues, December 2002 (GAO 2002 Report).

See for example, H.R. Rep. 106-655 (2000), which would require ISPs to terminate domestic Internet gambling merchants and to block foreign Internet gambling merchants upon request of law enforcement.

This system of coding and blocking Internet gambling transactions was described to Congress in a hearing before the House Financial Services Committee in 2001. See Testimony of Mark MacCarthy, Financial Aspects Of Internet Gaming: Good Gamble Or Bad Bet? Hearing before the Subcommittee On Oversight And Investigations Of The Committee On Financial Services U.S. House Of Representatives, July 12, 2001, No. 107-34, pp. 25-27 and 34-35. It is also described in the GAO 2002 Report, supra note 20.

The fines for incorrectly identifying authorization requests for online gambling transactions are set out at 1.6.D.7 of the Visa International Operating Regulations. In addition, Visa requires online gambling merchants to post certain notices: “…a Website for an Online Gambling Merchant must contain…the statement “Internet Gambling may be illegal in the jurisdiction in which you are located; if so, you are not authorized to use your payment card to complete this transaction. Visa International Operating Regulations at 5.4.C.2. The Visa rules are available at http://usa.visa.com/download/merchants/visa-international-operating-regulations.pdf.


10
11
12
13
14
15
16
17
18
19
20
21
22
Final Rule, p. 7. For similar reasons, the Agencies declined to develop, publish and update a list of merchants who were in violation of the Act. See discussion at p. 6.


The heart of Antigua’s case was that providers of gambling service located abroad could not provide the interstate horseracing gambling services that domestic U.S. providers could.

United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services - AB-2005-1 - Report of the Appellate Body, WT/DS285/AB/R, 05-1426, April 7, 2005. (Appellate Report), paragraphs 358-364. In 2005, a WTO Appellate Body issued a final ruling against the U.S. When the U.S. did not change its laws as ordered by the WTO, Antigua brought a compliance case. In March 2007, the U.S. lost that case, and Antigua was authorized to begin imposing sanctions. Antigua’s lawyers raised the option of lifting Antiguan compliance with WTO copyright rules relating to U.S. music and software. In May 2007, the U.S. gave notice to the WTO that it sought to withdraw “gambling and betting services” from WTO jurisdiction. Under WTO rules, a country may withdraw a service sector committed to WTO jurisdiction only with the authorization of other WTO signatory countries interested in the sector and only after compensating for future lost revenue a WTO signatory country might have earned were the commitment maintained. Goldsmith and Wu discuss the WTO case at pp. 172-173.

One attempt to resolve the issue was written into the statute. The agencies were required to ensure that transactions in connection with any activity excluded from the Act’s definition of “unlawful Internet gambling” are not blocked or otherwise prevented or prohibited by the prescribed regulations. See 31 U.S.C. 5364(b)(4). This appeared to exempt the horse racing industry, Indian gaming and intrastate gambling from the purview of the statute. The Agencies could have interpreted this to mean that the payments systems were required to process transactions that were not prohibited. They might have required the card systems to use special codes for transactions that are not prohibited by UIGEA. But the agencies declined to do these things. They determined that they did not have the authority to require card systems to process certain transactions and they left the creation of special merchant category codes to the business judgment of the card systems. See Final Rule, p. 20

They were given liability protection for this possible over blocking. See Final Rule p. 19.

Final Rule, p. 7,

31 U.S.C. 5365(a) and (b)

34 U.S.C. 5365(c). An interactive computer service has the same meaning as in section 230 of the Communications Decency Act of 1996, indicating that this provision has its roots in the same Internet exceptionalist thinking that generated that statute.

Google bans it. “Google has a zero-tolerance policy when it comes to child pornography and those who would promote it. Child pornography is illegal around the world and has no place in a civilized society. When we become aware of child pornography anywhere in our search engine index or on our site, we remove it immediately and report it to the appropriate authorities. We do not accept any advertising related to it. We cooperate assiduously with law enforcement authorities to help track down online criminals and child predators.” Testimony of Nicole Wong Associate General Counsel, Google Inc. before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, United States House of Representatives, June 27, 2006. Financial institutions also have a zero tolerance policy with respect to child pornography. Visa explicitly bans it from their payment system: “An Acquirer must both: ensure that a Merchant, Internet Payment Service Provider (IPSP), or Sponsored Merchant that displays a Visa-Owned Mark on its Website does not accept Cards for the purchase or trade of child pornography and terminate a
Merchant, IPSP, or Sponsored Merchant within 7 calendar days of Notification from Visa if the Merchant is identified as engaging in the purchase or trade of child pornography.” Visa International Operating Regulations at 4.1.C.5.b http://usa.visa.com/download/merchants/visa-international-operating-regulations.pdf. So does MasterCard. Its general rule against illegal transactions applies to “the sale of a product or service, including an image, which is patently offensive and lacks serious artistic value (such as, by way of example and not limitation, images of…sexual exploitation of a minor…” MasterCard Rules at 5.9.7 http://www.merchantcouncil.org/merchant-account/downloads/mastercard/MasterCard_Rules_5_08.pdf.

36 This account of Visa’s policies and procedures on child pornography is based on my Congressional testimony. MasterCard, American Express and PayPal have similar policies and procedures. See testimony of Mark MacCarthy, Arne Christiansen, Jodi Golinsky and Joe Sullivan at the Hearing Deleting Commercial Child Pornography Sites From the Internet: The U.S. Financial Industry’s Efforts to Combat This Problem before the Oversight and Investigations Subcommittee of the Committee on Energy and Commerce, U.S. House of Representatives, September 21, 2006

37 See testimony of Mark MacCarthy before the House Energy and Commerce Committee September 21, 2006, p. 69.

38 See testimony of Ernie Allen, President and CEO of the National Center for Missing and Exploited Children before the Committee on Banking U.S. Senate, September 19, 2006. (Senate Testimony of Ernie Allen)

39 See Testimony of Mark MacCarthy before the Committee on Banking, U.S. Senate, September 19, 2006.

40 See Senate Testimony of Ernie Allen, “We are seeing indications of a trend toward directing buyers away from credit cards and toward alternative payment methods to make the actual transaction.” See also his statement: “we are seeing that the credit card logos we are finding on these sites in most cases do not lead you to an actual account.” Testimony of Ernie Allen before the Oversight and Investigations Subcommittee of the Committee on Energy and Commerce, U.S. House of Representatives, September 21, 2006.

41 For example, Microsoft, Yahoo, and Google all require U.S. based pharmaceutical advertisers to be registered with PharmacyChecker. See PharmacyChecker at https://www.pharmacychecker.com/sealprogram/choose.asp “Google, Yahoo! and Microsoft adCenter require all advertisers and their affiliates who sell prescription drugs (as well as advertisers who refer visitors to prescription drug-selling sites) to be approved through the PharmacyChecker Verification Program. The advertised pharmacy must also be based in the U.S. or Canada.”

42 This description of policies and procedures used to combat controlled substances is based on my Congressional testimony. MasterCard has a similar program in place. See testimony of Mark MacCarthy and Michael McEneney at the hearing Safety of Imported Pharmaceuticals: Strengthening Efforts to Combat the Sales of Controlled Substances Over the Internet before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, U.S. House of Representatives, December 13, 2005.

43 Visa’s program shut down 49 similar sites. See testimony of Michael McEneney on behalf of MasterCard and Mark MacCarthy on behalf of Visa at the hearing before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, U.S. House of Representatives, December 13, 2005, p. 208.

44 See the testimony of Joseph Califano, on behalf of CASA, at the hearing Rogue Online Pharmacies: The Growing Problem of Internet Drug Trafficking before the Committee on the Judiciary, United States Senate, May 16, 2007. He summarizes the early studies as follows: “Over the four year course of our analysis, the number of selling sites has climbed steadily from 154 in 2004 and 2005 to 187 in 2007.”

45 National Center on Addiction and Substance Abuse at Columbia University, Press Release, “You’ve Got Drugs V” July 9, 2008: “The new White Paper reports that CASA researchers found a total of 365 Web sites advertising or selling controlled prescription drugs during 210 hours of research in the first quarter of 2008, compared to 581 sites during the same period in 2007/website.” The report noted that the” decline in the number of Web sites advertising or selling controlled prescription drugs may reflect efforts of federal and state agencies and financial institutions to crack down on Internet drug trafficking.” The large number of web sites offering to sell controlled substances does not indicate that all of them actually engage in that activity. CASA offered to Visa, MasterCard, American Express and PayPal a sample of 45 anchor sites from their analysis that offered to sell controlled prescription drugs and indicated that they accepted payment from one or more of these payment systems. Test transactions by the payment systems revealed
that only 4 of these sites actually attempted to process a transaction. The report acknowledges that this could be the result of “efforts made by these financial service providers to shut down use of their systems of payment for Internet trafficking.” See National Center on Addiction and Substance Abuse at Columbia University, You’ve Got Drugs V, July 9, 2008, p. 13.

For instance, Google does not accept online advertisements for tobacco products. See Content Policies for Tobacco and Cigarettes at https://adwords.google.com/select/contentpolicy.html “Advertising is not permitted for the promotion of tobacco or tobacco-related products, including cigarettes, cigars, tobacco pipes, and rolling papers.” (last visited on June 10, 2009.)

“Credit Card Companies Snuff Online Tobacco Sales.” Consumeraffairs.com, March 17, 2005


“MasterCard Urges Merchant Compliance with Rules Governing the Internet Sale of Tobacco”, Business Wire, March 8, 2005 at http://www.allbusiness.com/government/government-bodies-offices/5033201-1.html. “MasterCard said that financial institutions can continue to provide MasterCard acceptance for Internet tobacco sales if they have documented evidence to substantiate that the merchant is in compliance with all applicable federal, state, and local laws to the satisfaction of ATF and any applicable State Attorney General.”


See Settlement pp. 5-7


17 U.S.C. §512

A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001)

Perfect 10 v. Visa International Service Association, 494 F.3d 788 (9th Cir.2007) (Perfect 10) See Jonathan Band, "The Perfect 10 Trilogy," Computer Law Review International, October 2007 for a comprehensive discussion of this case and its relationship to similar secondary liability cases. He summarizes the Visa case as follows; “Here the Ninth Circuit rejected what would have represented a significant expansion of secondary liability to actors far removed from the infringing activity. However, unlike the other cases, this case provoked a strong dissent by respected jurist Alex Kozinski. This dissent suggests that the outer edges of secondary liability remain to be defined.” Judge Kozinski’s dissent is indeed stinging, but it also underestimates the burden that secondary liability would place on intermediaries.


This section describes the process at Visa, but other payment networks use a similar process.

IFPI’s role is discussed in my testimony before the Subcommittee On Courts, The Internet, And Intellectual Property. See also Nate Anderson, “Music industry encouraged Visa to pull the plug on AllofMP3.com,” ArsTechnica, October 18, 2006.


See testimony of Victoria Espinel, Assistant U.S. Representative for Intellectual Property and Innovation, Office of the U.S. Trade Representative testimony before the Subcommittee On Courts, The Internet, And Intellectual Property, Committee On The Judiciary, U.S. House Of Representatives International Piracy: The Challenges Of Protecting Intellectual Property In The 21st Century, October 18, 2007 at 30: “...we will continue to press Russia to shut down and prosecute the operators of illegal websites operating in Russia, including the successors to the infamous allofmp3.com.” See also United States trade Representative, Results of Bilateral Negotiations on Russia's Accession to the World Trade Organization (WTO): Action on Critical IPR Issues, November 19, 2006: “The United States and Russia agreed on the objective of shutting down websites that permit illegal distribution of music and other copyright works. The agreement names the Russia-based website allofmp3.com as an example of such a website.”


According to the IFPI, in May 2007 it “rated outside the top 2000 websites.” See IFPI “Police dawn raid stops allofmp3.com pirate vouchers scheme,” News Release May 21

Arbitration Court Of Moscow, Court Ruling in Case No. A40-70411/06-67-500, June 21, 2007 at p. 5: “According to Article 49 of the Russian Federation Law “On Copyright and Allied Rights”, it is only the Court that can execute actions in connection with illegal use of copyrights and allied rights, if there is a lawsuit filed by exclusive right holders, which the Defendants, VISA and IFPI are not, while in this case there are no court rulings with the force of res judicata establishing the Plaintiff’s illegal use of exclusive rights belonging to some right holders.” The Defendant was Rosbank, the Russian financial institution licensed by Visa to authorized merchants in Russia to accept Visa.

District Court of Moscow, Judgment in Case No. Case No. 1-151-07, August 15, 2007. See also testimony of Victoria Espinel before the Subcommittee On Courts, The Internet, And Intellectual Property, Committee On The Judiciary, U.S. House Of Representatives International Piracy: The Challenges Of Protecting Intellectual Property In The 21st Century, October 18, 2007 at p. 99: “My understanding of the case is that Media Services, the company that operated allTunes, was able to successfully argue in Russian court that it was not acting illegally because it was paying royalties to collecting societies, collecting societies that were not authorized by the rights holders.”

Indirect liability is not the same as holding a person responsible for the external negative effects of his own actions, but it has a resemblance. With a negative externality, a person engages in some action, such as cattle-raising or industrial production, and the spill over effects of that action harm some other party who is not directly involved in the activity. Cattle-raising might hurt the neighboring farmers and industrial pollution might harm innocent parties far and near. In this case, the responsible person’s actions are directly causing the harm. He is the bad actor. In the indirect liability case, the responsible person is in some fashion involved in the creation or maintenance of the harm and is also in a position to reduce the harm, either by detecting and deterring it or by reducing his own activity that contributes to it. But he is not the bad actor who is directly bringing about the harm. In a case of indirect copyright infringement, for
example, the bad actor is the infringer, while the third party would be some intermediary, an ISP or a payment system, whose activity or service allows the bad actor to commit the infringement.

78 Lichtman thinks his proposal for ISP liability for cyber security issues could be implemented in “negligence or strict liability, whether it is best implemented by statute or via gradual common law development…” Douglas Lichtman, “Holding Internet Service Providers Accountable,” Regulation Winter 2004, p. 59. Mann and Belzley suggest three possible regimes: traditional tort regime, a take down requirement and a hot list. Mann and Belzley pp. 22-24

79 Data security and notification statutes can be conceptualized as third party liability regimes which impose preventive and mitigation duties. The duty for a data controller to secure personal information under his control is designed to protect the data subject from potential wrongs perpetrated by data thieves. The duty to notify a data subject of a security breach when there is a reasonable likelihood of identity theft or other harm is intended to provide the data subject with information that he can use to protect himself from these harms. A further example of an indirect liability scheme in the data security area is the Minnesota cost recovery statute that holds merchants liable for the costs association with a breach when they failed to take specific precautions that are part of an industry data security standard. Minnesota’s law specifies that “No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction” See 325E.64 Subdivision 2 at https://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP&year=2007&section=325E.

This precaution of not saving authentication codes is based on the PCI DSS industry standard. The law goes on to state: “Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person’s or entity’s service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders…” See 325E.64 Subdivision 3 at https://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP&year=2007&section=325E.

80 Some privacy requirements can also be thought of as third party liability regimes. Data controllers have a duty to protect the accuracy and integrity of the personal information under their control (for example, by making sure that it is up to data and current and by responding to data subject complaints of inaccuracy) in order to protect data subjects from harm by third parties who obtain this information from data controllers and use it for eligibility decisions (such as employment, credit or insurance).

81 Some consumer protection requirements in the financial services industry are also usefully viewed as third party liability regimes. Financial institutions participating in the provision of payment card services are required under Federal law to protect cardholders in various ways: they must investigate and promptly correct billing errors that consumers allege have occurred in connection with their accounts; consumers are eligible to maintain against a creditor much the same claims that they might assert against a merchant in connection with the purchase of defective or otherwise unsatisfactory goods and services; the law limits a consumer’s liability for an unauthorized use of payment cards. These regulations oblige financial institutions to step in to protect cardholders against harms such as improper billing, fraud or non-delivery of goods by merchants who are linked together with cardholders in a payment system. They also oblige financial institutions to protect cardholders from financial harms by fraudsters in connection with the fraudulent uses of payment cards. The Truth in Lending Act (Pub. L. No. 90—321; 15 U.S.C. 1601) was originally passed by Congress in 1968. Major amendments to TILA were made by the Fair Credit Billing Act of 1974, the Consumer Leasing Act of 1976, and the Truth in Lending Simplification and Reform Act of 1980. The Board of Governors of the Federal Reserve System implemented these requirements through Regulation Z. The implementation through Regulation Z is found at 12 CFR226.12. The Electronic Funds Transfer Act (Pub. L. No. 96-630; 15 U.S.C. § 1693 et seq.) was passed by Congress in 1978. The Board of Governors of the Federal Reserve System implemented these protections through Regulation E. Regulation E can be found at 12CFR205. Regulation E does not provide remedy for a consumer who has purchased allegedly defective goods or services using a debit card.

82 47 U.S.C. §230(c)(1). See the discussion of the extension of this immunity in Holland pp. 105-108.

83 17 U.S.C. §512(a) and (c)-(d).
The court ruled that eBay exerted sufficient control to evaluate for contributory liability, and then found that their procedures satisfied the requirements of taking action when they knew or should have known of specific acts of infringement. “Nevertheless, under the law as it currently stands, it does not matter whether eBay or Tiffany could more efficiently bear the burden of policing the eBay website for Tiffany counterfeits — an open question left unresolved by this trial. Instead, the issue is whether eBay continued to provide its website to sellers when eBay knew or had reason to know that those sellers were using the website to traffic in counterfeit Tiffany jewelry. The Court finds that when eBay possessed the requisite knowledge, it took appropriate steps to remove listings and suspend service. Under these circumstances, the Court declines to impose liability for contributory trademark infringement.” eBay p. 2-3 Oral arguments in the appeal to the Second Circuit were held on July 16, 2009

See H.R.1166, the E-Fencing Enforcement Act of 2009. It requires an online market provider to deny high volume sellers access to the marketplace if he has good reason to believe that such they acquired their goods unlawfully.


The effective reach condition is phrased as prior to an assessment of the ability of a third party to effectively control the bad activity. If the law or the wronged party can easily reach the bad actor, then why even consider whether to impose a duty on a third party? Of course, the bad actors are never totally out of reach of the law or wronged parties. With some finite expenditure of resources, perhaps very large, the direct bad actors could be brought to justice or harms prevented. The real economic question is whether those costs are larger than the costs of assigning that enforcement role to a third party. And this means that the effective reach condition collapses into the control factor discussed later. Landes and Lichtman at p. 398 put the comparative point accurately, applied to the specific case of contributory copyright liability, as follows: “Holding all else equal, contributory liability is more attractive…the greater the extent to which indirect liability reduces the costs of copyright enforcement as compared to a system that allows only direct liability.”

Lichtman and Posner, p. 16. They also seem to starting in the right place with their focus at p. 42 on what the parties might do: “The right thought experiment is to imagine that all the relevant entities and all the victims and all the bad actors can efficiently contract one to another, and then ask how the parties would in that situation allocate responsibility for detecting and deterring bad acts.” But there is no need to conduct this thought experiment in the abstract. Free, equal, and rational parties can bargain to allocate responsibility and so we can answer the question of what the parties would do in this thought experiment by looking at what they actually do. The relevant inquiry is whether the bargaining situation is free of significant transaction costs or other obstacles to reaching an agreement.


For example, Lichtman and Posner express some puzzlement as to why the parties haven’t worked out liability arrangements in their discussion of ISP liability for security flaws. Lichtman and Posner, p. 14-17. This fact could mean that there are no mitigation efforts that intermediaries can undertake that would effectively avoid damages at a price that the wronged parties are willing to pay. It could mean that that transaction costs are so high that intermediaries and wronged parties cannot reach efficient arrangements. It could mean that perceptions of equities prevents the parties from reaching a rational accommodation, in the same fashion that parties to the “ultimatum” game in behavioral economics reject advantageous but unfair low-ball offers (See James Surowiecki, The Wisdom of Crowds, Doubleday, 2004 pp. 112-113 for a description of the ultimatum game). Or it might mean that the wronged parties are counting on changes in legal liability that would require intermediaries to take enforcement efforts at their own expense. Lichtman and Posner seem to starting in the right place with their focus at p. 42 on what the parties might do: “The right thought experiment is to imagine that all the relevant entities and all the victims and all the bad actors can efficiently contract one to another, and then ask how the parties would in that situation allocate responsibility for detecting and deterring bad acts.”

Testimony of Mr. Robert Chesnut, Senior Vice President, Rules, Trust and Safety, eBay,

93 See Mann and Belzley p. 30: “In a perfect world of course the baseline would be irrelevant because the trademark owner would negotiate to purchase a takedown from eBay if that were an efficient outcome. Here, there is some reason to think that might happen, where transaction costs between two large companies are low when compared to the value of the rights being negotiated.”

94 The District Court in the eBay case wrote: “In effect, Tiffany’s contributory trademark infringement argument rests on the notion that because eBay was able to screen out potentially counterfeit Tiffany listings more cheaply, quickly, and effectively than Tiffany, the burden to police the Tiffany trademark should have shifted to eBay. Certainly, the evidence adduced at trial failed to prove that eBay was a cheaper cost avoider than Tiffany with respect to policing its marks.” eBay p. 56. But if Tiffany thought that eBay could take enforcement action “more cheaply, quickly and effectively than Tiffany” why didn’t they negotiate arrangements with eBay to do that? The fact that they didn’t should be at least relevant evidence that their own efficiency argument is mistaken and that they are really relying on an equity argument: that eBay should be forced to pay for enforcement actions that are not commensurate with Tiffany’s gains because it is their responsibility to do so.

95 The House Judiciary Committee held a hearing on an earlier version of this legislation. See testimony by Edward Torpoco, Senior Regulatory Counsel for eBay before the Committee on the Judiciary, U.S. House of Representatives, September 22, 2008 to get a sense of how this legislation might affect an online marketplace like eBay. He emphasizes at p. 6 his concern that the bill would violate a fundamental legal principle that Internet service providers like eBay “should not be held liable for content posted by third parties.”

96 Testimony of Mr. Joseph J. LaRocca, Vice President, Loss Prevention, National Retail Federation, before the Committee on the Judiciary, U.S. House of Representatives, September 22, 2008, p. 46. It is hard to avoid the conclusion, voiced by Steve DelBianco on behalf of the online marketplaces at p. 42 of the same hearing that “retailers would understandably say, we are not ready to sign up for a voluntary program if someone is dangling in front of us legislation that creates a club... in the form of being able to demand the interrogation of customers without any law enforcement being involved.”

97 Several commentators seem to stop with the “good position” analysis. See Lichtman and Posner at p 4: “Our argument in favor of service provider liability is primarily based on the notion that Internet service providers are in a good position to reduce the number and severity of bad acts online.” Landes and Lichtman at p. 409 make a similar argument regarding Internet intermediaries: “…although these parties are only indirectly responsible, they are typically in a good position to either prevent copyright infringement or pay for the harm it causes.”

98 There is an extensive law and economics literature in this area. See Mann and Belzley for a summary. See also Ward Farnsworth, “The Least Cost Avoider,” pp. 47-56 in The Legal Analyst, University of Chicago Press, 2007. The term “least cost avoider” was coined by Guido Calabrese in The Costs of Accidents Yale University Press, 1970

99 For the clearest argument in favor of intermediary liability based on this least cost avoider perspective, see Mann & Belzley. Other defenders of the least cost perspective are: Michael L. Rustad & Thomas H. Koenig, “Rebooting Cybertort Law,” 80 Washington Law Review 335; Joel R. Reidenberg, “States and Internet Enforcement,” 1 University of Ottawa Law and Technology Journal 213 (2003).

100 If there are fewer Internet subscribers then the service is less valuable to ecommerce merchants as well since there are fewer potential customers. See Matthew Schruers, “The History And Economics Of ISP Liability For Third Party Content,” 88 Virginia Law Review 205 (2002) (Schruers), pp. 250-252. See also Lichtman and Posner pp. 23-25. They seem to minimize the importance of these external, network effects in assessing liability regimes at 25: “Immunizing ISPs from liability is not the correct mechanism for encouraging them to provide positive externalities.” However, the loss of the ISP generated external benefits is a potential cost of assigning liability that has to be taken into account when assessing whether to assign liability. Mann and Belzley at p. 28 gets the overall point right, noting: “To the extent the regulation affects conduct that has positive social value—as it is likely to do in at least some of our contexts—the direct and indirect effects on that conduct must be counted as costs of any regulatory initiative.”
See, for example, Mann and Belzley at 24-25: “It should be plain that the liability schemes that we envision are not the type of thing readily adopted through the development of the common law. Our framework is intended to provide fodder for legislators and regulators, not for judges. Thus, we hope that our analysis can lead to well-specified statutory schemes or regulatory initiatives.”

See, for example, the district court decision in the eBay case: “...even if it were true that eBay is best situated to staunch the tide of trademark infringement to which Tiffany and countless other rights owners are subjected, that is not the law.” eBay at p. 56

Oral arguments in the appeal to the Second Circuit were held on July 16, 2009

The least cost analysis seems to function like a cost effectiveness analysis, where a given level of enforcement is assumed and the question is how that goal can be reached at the lowest cost. Mann and Belzley seem to adopt that perspective at p. 8: “…a mature scheme of regulation that limits the social costs of illegal Internet conduct in the most cost-effective manner.” But a full cost-benefit analysis gives up the assumption of a fixed benefit goal and takes the value of benefits into account as well.

Lichtman and Posner, p. 12. Lichtman and Landes illustrate at 404-405 how this “activity” factor works in discussing, “an instance where it would be prohibitively expensive to distinguish legal from illegal copyright activity,” and appear to conclude that “Internet service providers are a good example in this category.” But then they note that perhaps they should still be liable in this case: “After all, instead of trying in vain to distinguish lawful from unlawful activity, a firm in this situation would simply increase its price and use that extra revenue to pay any ultimate damage claims. Legal liability, then, would function like a tax. In many instances such a tax would be welfare reducing in that higher prices discourage legal as well as illegal uses. But in some settings, discouraging both legal and illegal activity would yield a net welfare gain. This would be true where illegal behavior is sufficiently more harmful than legal behavior is beneficial; it would be true where the harms and benefits are comparable but illegal behavior is more sensitive to price; and it would be true where the benefits in terms of increased copyright incentives outweigh the harms associated with discouraging legitimate use”

The factual issues raised by an activity tax that reduces all use of the intermediary facilities, legal and illegal, is connected to the over breadth of a measure apparently targeting just illegal activity. In February 2002, the Pennsylvania legislature enacted a law that imposes potential liability on Internet Service Providers for child pornography available anywhere on the Internet. In Center For Democracy & Technology V. Pappert Case No. 03-5051 (E.D. Pa. Sept. 10 2004), the District Court for the Eastern District of Pennsylvania struck down the law on First Amendment grounds, ruling that it impermissible chilled legitimate speech by blocking legitimate websites (as many as 1 million) as well as child pornography sites. This case could be viewed as a judicial review of the activity tax idea, where the harm imposed by the overall reduction in legitimate Internet usage outweighed the benefit of reduced access to child pornography sites. It also indicates that indirect liability regimes need to be evaluated in comparative fashion. Alternative methods such as voluntary efforts to block payments to child pornography sites need to be examined as well. Landes and Lichtman at pp. 20-22 reject the activity factor rational for imposing cyber-security liability on ISPs.

See Landes and Lichtman at p. 408 “…like any legal issue, these questions about the relative virtues of indirect liability have to be evaluated dynamically.”

For instance, putting liability on cardholders for fraud losses would not create an incentive to innovate improvements in fraud prevention. There is almost nothing individuals can do to change their behavior to reduce fraud. However, when financial institutions have to bear the liability, they have every incentive to reduce fraud through the use of new innovative technologies, and they are well positioned to develop and introduce such technologies into payment systems. The neural networks that currently catch fraud almost in real time are a result of this allocation of liability. Fraud in payment systems has been dropping over time, from around 20 basis points in the 1980s to 5 or 6 in 2007 and 2008.

The effect of the liability rules set out for the payment card industry greatly increased consumer confidence in using the innovative new technology; consumers could use payment cards without worrying that they would be liable for fraud. It is likely that the dramatic growth in the industry in the 1980s and 1990s was attributable to the widespread impression among consumers that using this new technology was safe, and the immunity from liability helped create that consumer confidence.

Landes and Lichtman make reference to this infant industry argument at p. 406 and 409. Mann at p. 16 appears to be critical of it, arguing that exemptions from liability for pure Internet actors derive from “the
reflexive and unreflective fear that recognition of liability for intermediaries might be catastrophic to Internet commerce…”

110 See Mann and Belzley p. 7. Their idea at p. 16 is that “the intermediaries might be the most effective sources of regulatory enforcement, without regard to their blameworthiness.” And they call their proposal “liability without fault.”

111 They also treat the least cost standard as a legal litmus test. Being the least cost avoider is necessary and sufficient for indirect liability. No other standard or consideration intervenes to affect the analysis. As we have seen, that standard leaves out the benefits part of the equation and is too limited.

112 Any introductory account of the philosophical problems associated with utilitarianism makes this point. See, for example, Jonathan Wolff An Introduction to Political Philosophy Oxford University Press 1996 p. 57: “….utilitarianism will permit enormous injustice in the pursuit of the general happiness.” A more sophisticated indirect or rule utilitarian approach can attempt to meet this difficultiy, but that approach is subject to difficulties of its own. See the general critique of utilitarianism in John Rawls, A Theory of Justice Harvard University Press 1971. The underlying intuition behind this alternative account of social justice at p. 3 is that “each person possesses an inviolability founded on justice that even the welfare of society as a whole cannot override.” Rawls also notes that public policies have to defensible publicly in order to be legitimate. This publicity principle makes it very difficult for liability to be assigned to third parties without a finding of blameworthiness.

113 See Jim Harper, “Against ISP Liability” Regulation, Spring 2005 pp. 30-31, arguing that ISPs should be liable for harms to third parties only if they have a duty to these parties and that “efficiency” considerations do not override the lack of a such duty founded on justice. Libertarians generally reject the idea that we have positive duties to ameliorate harms we did not cause.

114 See, for instance, Judge Posner’s discussion of good Samaritan law in Stockberger v United States 332 F.3d 479 (2003) and repeated in Cuyler v. United States 362 F.3d 949 (2004). Mann and Belzley at p. 25 note that the principle that liability should be assigned regardless of blameworthiness “easily could shade into judicial doctrines that would obligate all actors to stop all misconduct whenever they can.” They cite Judge Posner’s objection to this “unbounded principle” as “unduly disruptive.” But it is hard to see how their proposal to implement liability through regulation would be less disruptive.

115 See, for example, Thomas Pogge “Cosmopolitanism and Sovereignty,” in World Poverty and Human Rights, Blackwell, 2002, pp. 168-195, especially p.172, where he argues that those involved in an institutional order that authorizes and upholds slavery have a duty to protect slaves or to promote institutional reform, even if they do not own slaves themselves.

116 See, for example, David Luban, “Just War and Human Rights,” in International Ethics, edited by Charles Beitz et al. Princeton University Press 1985, p. 209, where he says that “all humans in a position to effect” a human right have an obligation to do so.

117 Mann and Belzley at p. 16 criticizes the “myopic focus on the idea that the inherent passivity of Internet intermediaries makes it normatively inappropriate to impose responsibility on them for conduct of primary malfeasors.” But passivity is relevant to the knowledge and control factors needed to assess liability from an equity point of view. Landes and Lichtman at 405 seem to criticize the focus of current law on “knowledge, control, the extent of any non-infringing uses, and other factors” because they are not “particularly clear as to why those issues are central.” But these factors are crucial because they related to the way in which the equity issues can be resolved.

118 These equity considerations can interact with the cost analysis. Consider the following: suppose transaction costs make it impossible for the wronged parties to negotiate enforcement deals with a third party – they are too numerous or lack the resources to compensate the third party. Suppose further it is possible that the cost savings involved in assigning liability to a third party is substantial. And finally stipulate that the third party’s involvement in the harm is so remote that assigning blame is a mistake. We might in that circumstance nevertheless assign liability to the third party. The gains to the rest of us are just too great. However, shouldn’t we compensate the third party for taking the enforcement steps he is required to take? Assigning indirect liability when there isn’t this level of control or fault to justify blameworthiness might be so efficient under a cost analysis that it is worth considering, but in that case the use of compensation mechanisms should also be considered.

119 Lichtman and Posner, p. 12

120 Perfect 10 at 7888. See also his comment: “…the complaint alleges that defendants are not merely passive providers of services available on equal terms to legal and illegal businesses alike; they are actually
in cahoots with the pirates to prop up their illegal businesses and share their ill-gotten gains.” Perfect 10 at 7881. This allegation turns on what I think is a factual mistake - that the higher prices that adult content merchants pay for accepting cards is an attempt to share their ill-gotten gains rather than an attempt to compensate for the extra credit risk these merchants impose on the system. But the normative tone is unmistakable.

121 The Kozinski dissent is typical in this regard.


124 Perfect 10 p. 7889

125 League Against Racism and Anti-Semitism (LICRA) versus Yahoo, Interim Court Order, County Court of Paris, November 20, 2000. In this particular example, other countries probably would not need to use financial institutions, since most online entities including Yahoo have taken steps to prevent the shipment of Nazi paraphernalia to countries that ban them.

126 See Mann and Belzley p. 29: “Surely eBay is more adept at searching and monitoring its marketplace than Tiffany & Co.; at the same time, eBay probably is not as effective as Tiffany & Co. is at the task of distinguishing bona fide Tiffany products from counterfeits.” See also Schruers at 252: “...the ISP is not the least-cost avoider when it comes to discovering (illegal) content; it is only well suited for cost avoidance after it is apprized of the problem.” And he adds that in this case, the wronged party may be better suited to the task of locating the offending content.

127 Mann and Belzley at p. 26. They have a useful discussion of this over blocking issue: “There always is the risk that imposing additional burdens on intermediaries can chill the provision of valuable goods and services. That will be especially problematic in cases in which there is considerable risk of chilling legal conduct that is adjacent to the targeted conduct. As we discuss below, that might tend to make the use of intermediaries less plausible in file-sharing contexts (where it is quite difficult to be sure any particular act of file-sharing is illegal) and much more plausible in the gambling context (where it is plausible in many cases that substantially all traffic to a particular site involves illegal conduct). Requiring intermediaries to make those kinds of subjective decisions imposes costs not only on the intermediaries (that must make those decisions), but also on the underlying actors whose conduct might be filtered incorrectly.” The Internet gambling case illustrates that determining when a particular website is engaged in illegal gambling is not a simple task. It is fraught with just the kind of “subjective decisions” that Mann and Belzley are properly concerned about. The actual experience of payment systems in the face of this difficulty is not to make these subjective decisions, but to block all gambling activity, including legal gambling transactions.

128 Letter from Representative Barney Frank, Chairman of the House Financial Services Committee, to Hank Paulson, Secretary of the Treasury, November 10, 2008. The text of the letter is at http://www.house.gov/apps/list/press/financialsvcs_dem/11102008.shtml. Chairman Frank introduced legislation (HR 5767, later HR 6870) that would have prohibited the implementation of these flawed rules and would have replaced them with a formal rulemaking process that would define the term “unlawful Internet gambling,” something the proposed rules fail to do. HR 6870 was passed by the Financial Services Committee on September 16, 2008. But the Agencies issued their final rules in December 2008.


130 Mann and Belzley at p. 15 note that “…regulators in a variety of contexts have reached informal agreements with intermediaries in which intermediaries voluntarily agree to cooperate. Our impression is that most of those agreements do not reflect the view of the intermediaries that they could be forced in litigation to provide that cooperation, but rather the view that a failure to cooperate would result in formal legislative regulation; the settlements proceed not in the shadow of existing law, but in the shadow of potential law.” But if the pressure to cooperate “in the shadow of potential law” has worked, why actually legislate?


133 H. R. 1076 Section 3 at http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.1076. The Center for Democracy and Technology describes the problem with this approach. “The problem is that any major
national service provides knows – as almost a statistical certainty – that someone is using their services to “facilitate” access to child pornography.” See Center for Democracy and Technology Analysis of H.R. 107, June 2009.

134 See H.R. 1076 Section 5. CDT’s analysis of this provision notes the difficulties record retention would create for Internet service providers and the tension with privacy concerns.


136 See Sections (h)(1)(B) and (h)(2)(C)

137 See Sarah Rubenstein, “New Bill Targets Rogue Druggists on the Internet,” Wall Street Journal, October 9, 2008. “Finally, the bill does not create new requirements for Internet search engines, credit-card companies or package-delivery concerns whose services are used in online pharmacy transactions.”

138 See Section (h)(3)(A)(iii)

139 In the area of controlled substances, some groups have called for mechanisms to supplement the efforts of third parties with a special government-funded monitoring entity. This monitoring entity would send information to payment card companies and other intermediaries, which would then trigger an automatic legal requirement to investigate and block. See for example, the testimony of Professor Philip Heymann, on behalf of the "Keep Internet Neighborhoods Safe" (KINS) initiative, based at the Center for International Criminal Justice at Harvard Law School, at the hearing Rogue Online Pharmacies: The Growing Problem of Internet Drug Trafficking before the Committee on the Judiciary, United States Senate, May 16, 2007.

This is a system of indirect liability with the obligation to act triggered by the activity of a non-governmental private party. It is not necessary and would not improve the efficiency of the existing monitoring system. Centralizing the monitoring function in cooperation with law enforcement, however, would create some savings.


141 See Perfect 10 at 7889: “Credit cards already have the tools to police the activities of their merchants, which is why we don’t see credit card sales of illegal drugs or child pornography.” Of course, card companies use different tools in the case of illegal drugs and child pornography, namely, proactive monitoring, but it is hard to see on Kozinski’s analysis why card companies shouldn’t use whatever tools they can to stop illegal activity in all cases. See also Perfect 10 at 7889: “Plaintiff is not asking for a huge change in the way credit cards do business; they ask only that defendants abide by their own rules and stop doing business with crooks. Granting plaintiff the relief it seeks would not, I am confident, be the end of Capitalism as we know it.” But it might be the end of payment systems as we know them if indirect liability for them means an obligation to stop doing business with everyone who might be involved with illegality anywhere. He attempts at 7881 to limit his analysis to those cases where there are special arrangements between bad actors and the payment system, but nothing in his analysis turns on these special arrangements. These special arrangements turn out to be risk-based pricing for adult content websites. Would he really have voted with the majority if the price that adult content merchants face for accepting cards was the same as the price set for less risky merchants?

142 Perfect 10 at 7876

143 Perfect 10 at 7887. “Credit cards already have the tools to police the activities of their merchants, which is why we don’t see credit card sales of illegal drugs or child pornography.”

144 Perfect 10 at 7889

145 Mann and Belzley’s argument at p. 18 on Perfect 10 also seems mistaken. “In terms of equity, Visa has clean hands and Cybernet does not. That might make sense in a legal system designed to force bad actors to provide redress to injured parties. The better question, however—albeit one not readily susceptible of judicial analysis—is whether either Visa or Cybernet is the party best situated to stop the copyright violations in question. On that point, Visa probably is much better situated, because of the real-world likelihood that none of the sites that fosters the infringement could survive as a profitable commercial enterprise if it could not accept payments from Visa.” Several points need to be made. The equity considerations cannot be ignored. If Visa has “clean hands” it is hard to see why they should be held responsible. Also, the fact that Visa is better positioned than some other party to take enforcement action does not imply that these enforcement costs are worth the benefits. And the existence of complaint procedures suggests that indirect liability is not as a practical matter required.
See Results of Bilateral Negotiations on Russia's Accession to the World Trade Organization (WTO): Action on Critical IPR Issues: “Russia will work to enact legislation by June 1, 2007, to stop collecting societies from acting without right holder consent; Russia will also work to enact legislation implementing the 1996 World Intellectual Property Organization (WIPO) Internet treaties.” These new measures might enable Russian courts to reverse their earlier decisions. See testimony of Victoria Espinel before the Subcommittee On Courts, The Internet, And Intellectual Property, Committee On The Judiciary, U.S. House Of Representatives International Piracy: The Challenges Of Protecting Intellectual Property In The 21st Century, October 18, 2007 at 30.


Johnson and Post

Johnson and Post, p. 1370

Johnson and Post, p. 1375

Johnson and Post, p. 1376

Mann and Belzley at p. 8 describes their view as “consciously exceptionalist” because “specific characteristics of the Internet make intermediary liability relatively more attractive than it has been in traditional offline contexts: the ease of identifying intermediaries; the relative ease of intermediary monitoring of end-users; and the relative difficulty of direct regulation of the conduct of end-users.” But this is an odd way of framing the issue. Internet exceptionalism is not simply the view that the Internet should be treated differently from the offline world. The claim is more specifically that the Internet should be free of local jurisdictions. Mann’s view, which implies that the Internet should be brought under local jurisdictions through the mechanism of intermediary liability, is thus the very opposite of exceptionalism. It is one version of Internet non-exceptionalism.


Goldsmith and Wu, p.68

Goldsmith and Wu, p. 140

Lawrence Lessig, Code And Other Laws Of Cyberspace Basic Books, 1999

See Holland pp. 108-119 for a summary of this way of connecting the Internet exceptionalist debate with the net neutrality debate.

Against Cyberanarchy, p. 1236

On the Internet it is “easier for even solvent malfeasors engaged in high-volume conduct to avoid responsibility either through anonymity or through relocation in a jurisdiction outside the influence of concerned policymakers.” Mann and Belzley at p. 15. They also argue at p. 28 that indirect liability makes sense in “cases in which the retailer is located outside the United States, in a jurisdiction that will not cooperate with the applicable state regulators.”

Goldsmith in Against Cyberanarchy discusses many of these theories. See also the summary of these theories in Paul Schiff Berman, “Choice Of Law And Jurisdiction On The Internet: Towards A Cosmopolitan Vision Of Conflict Of Laws: Redefining Governmental Interests In A Global Era,” University Of Pennsylvania Law Review, Vol. 153, p. 1819, 2005. (Berman)


The European Union appeared to take the side of the country of origin in its ecommerce directive. The Ecommerce directive contains an Internal Market clause which means that “information society services are, in principle, subject to the law of the Member State in which the service provider is established.” See summary at http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

In 1999, the OECD issued its Guidelines for Consumer Protection in the Context of Electronic Commerce, which address principles that could be used by electronic commerce merchants in the absence of global consumer protection rules. The FTC and the OECD are holding at 10th year anniversary of the release of these guidelines in December 2009.

In an interesting twist, some commentators used the presence of these dispute resolution mechanisms to argue against indirect liability for intermediaries. Why deputize intermediaries to stop illegal activities on the Internet, when governments can reach the bad actors and resolve any disputes in the normal way? Responding to the argument that indirect liability is needed because the bad actor is unreachable by law enforcement or aggrieved parties, Holland at p. 125 says: “As an initial matter, it is not clear that a significant number of bad actors are beyond the reach of the law. Advances in technology are making it...
increasingly possible to locate and identify bad actors online, such that online anonymity is difficult to maintain. Likewise, where the bad actor is identified but is found outside the jurisdiction, sovereign governments have developed methods for resolving disputes to permit the direct extraterritorial application of domestic law, such as rules of jurisdiction, conflicts of laws, and recognition of judgments.

165 Berman at p. 1862. His work has affinities with that of political philosophers working in the area of national sovereignty in a global world. See, for example, Thomas Pogge, “Cosmopolitanism and Sovereignty,” in World Poverty and Human Rights, Blackwell Publishers, 2002, pp. 168-195

166 Visa’s policy is stated in my testimony before the Subcommittee On Courts, The Internet, And Intellectual Property, Committee On The Judiciary, U.S. House Of Representatives International Piracy: The Challenges Of Protecting Intellectual Property In The 21st Century, October 18, 2007. Other payment intermediaries have similar procedures. eBay has a similar restriction about selling and shipping illegal goods to the country where they are illegal. For example: “...because eBay is a worldwide community, many of our users live in countries where the possession or sale of items associated with hate organizations is a criminal offense. We can't allow the sale or shipping of these items there.” See the eBay offensive material policy at http://pages.ebay.com/help/policies/offensive.html

167 The internal application of this rule involves system efficiency and the balance of interests among the stakeholders in the system. If the merchant is in violation of its own country’s law, then enforcement is conceptually easy. Merchants discovered in violation of local law either have to stop the transactions or be removed from the system. If the merchant is in violation of the law in a different jurisdiction, things are more complicated. Should the bank of the merchant or the bank of the customer be burdened with the enforcement responsibility? If the merchant has this responsibility, then he must not introduce the illegal transaction into the system and the merchant’s bank must not try to process it, then steps must be taken at the merchant’s end to stop the transaction. These steps could include: a system decision requiring the merchant to stop these transaction entirely or leave the system, or coding and programming modifications by the merchant, the merchant’s processor, or the system operator, that would block transactions at the merchant end from entering the system if the customer was from a jurisdiction where the transaction would be illegal or which would restrict the transaction to the merchant’s own jurisdiction. Alternatively, the enforcement measures could be put on the cardholder side. Merchants could introduce properly coded transactions into the system and rely on action on the cardholder’s side to stop the transaction. This seems to fit the case of Internet gambling, where U.S. law makes Internet gambling illegal for US citizens, and the payment networks responded to UIGEA with a coding and blocking system that allowed merchants to continue their services in countries where Internet gambling was illegal. For instance, should merchants be responsible for knowing the laws of all the countries of all the customers they deal with? Perhaps not, but if 90% of their sales are from an offshore jurisdiction, they should be responsible for knowing that sales of their product are legal in that jurisdiction. Violations of the policy would largely be dealt with on a complaint basis.

168 See for example the case of SWIFT, where SWIFT was required to comply with US demands for access to financial information about European customers in virtue of its operations on US soil, while such compliance put them in violation of the European data protection directive. In addition, passage of the Global Online Freedom legislation (GOFA) could put Internet intermediaries in a conflict of law situation with China and other countries. See H.R. 275 introduced by Representative Chris Smith January 5, 2007. GOFA would require U.S. intermediaries to resist certain orders from countries in which they are doing business. The US Patriot Act also apparently put Canadian affiliates of US companies is the awkward position of needing to supply information about Canadian citizens to US law enforcement in ways that many thought violated the Canadian privacy laws.

169 Antigua brought a complaint against the US for the enforcement of its gambling laws, but its success was based only on (1) the US’s failure to exclude Internet gambling from the list of services that required open treatment and (2) the idiosyncrasies of US gambling law which appear to allow domestic horse racing to engage in Internet gambling while denying similar opportunities to offshore Internet gambling merchants. But these are technical obstacles created by the interaction of complex US law and international WTO law and are not real conflict of law problems.

This is based on transaction data from the Visa system. See statement of Mark MacCarthy before the Subcommittee on Courts, the Internet and Intellectual Property of the Committee on the Judiciary, U.S. House of Representative, October 18, 2007, at p. 3.


See Post Against Against at p1377 “scale matters.” See also Holland Failure at 29: “The online actor cannot know, as a practical matter, the many laws applicable to a particular act, nor when one or more sovereign may decide to attempt regulatory action. This is particularly true in those areas of regulation in which morality, religion and culture are at their most influential, such as speech, race, sex, and even intellectual property. Moreover, it is not simply one actor or a few legal systems. It is an exponential multitude.”

See Goldsmith and Wu, p. 160, where they suggest that acting as the Internet police is just a normal cost of doing business for global companies, which they can avoid in a particular case by leaving a country that tried to impose costs that exceeded the benefits of continued presence in the country. This creates another objection to the bordered Internet: it effectively gives larger countries a greater role in Internet governance than smaller ones.

Holland, p. 119.

Holland, p. 120: “The dramatic expansion of § 230 immunity has effectuated many of the ideals promoted by Post, Barlow, and others, albeit on a limited scale. This expansion has created an environment in which many of the norms and regulatory mechanisms present in the offline world are effectively inapplicable. This is so not because the very nature of cyberspace makes such application impossible, or because sovereign law is necessarily ineffective or invalid, but rather because sovereign law has affirmatively created that condition.”

Holland pp. 123-130

Holland pp. 130-136

Holland p. 130

Holland p. 132. See also Schruers at p. 261: “ISP respond to content-based complaints as a matter of good business practice for the purpose of maintaining customer goodwill and satisfaction.”


Brad Stone, “Under Pressure, Craigslist to Remove ‘Erotic’ Ads,” New York Times, May 13, 2009. Craigslist attorney’s asserted immunity under section 230, but chose voluntarily to remove the ads that various state attorneys general had objected to. State Attorney’s General felt confident that they could bring a case under state criminal law despite the immunity granted by section 230. The case was given national attention when a medical student was accused of killing a masseuse whom he met through Craigslist.

See Johnson and Post, p. 1380 for a description of AOL or Compuserve terms of service as examples of law in cyberspace. Their view at p. 1388 is that the rules for an Internet community should be “a matter of principled discussion, not an act of will by whoever has the power switch.” But it is hard to see how terms of service for a typical Internet service or application is anything other than an act of will by the person who controls. It might satisfy certain legal standards for informed consent, but it is not the product of principled discussion.


The antitrust issue is relevant to the original exceptionalist vision of the evolution of Internet communities. If these communities tend toward concentration, then the ability of some communities to dominate others is present. Individual community level norms cannot protect the more vulnerable communities in that context and the result might prevent the smooth emergence of viable and attractive rule sets that cannot gain a foothold in the Internet ecology because of the established presence of dominant communities. Yochai Benkler discusses many of these “concentration” issues in The Wealth of Networks Yale University Press, 2006 at pp. 235-272. But see the critique by Matthew Hindman, “What is the Online Public Sphere Good For?” in Joe Turow and Lokman Tsui, eds., The Hyperlinked Society University of Michigan Press, 2008.

an advertising service that allowed a user’s online activities to be distributed to other community members. In the face of this protest, it provided a simple way for users to decline to participate.

See the summary of these developments on the EPIC Social Networking Privacy page at http://epic.org/privacy/socialnet/default.html (last visited on July 8, 2009).


188 In the Sears case they obtained a settlement from Sears after charging that their consent practices in regard to installing an online tracking program on customers’ computers constituted an unfair or deceptive practice. See Federal Trade Commission, Sears Settles FTC Charges Regarding Tracking Software Press Release, June 4, 2009.

189 David Vladek, the new head of the FTC’s consumer protection division, is rethinking privacy. He says that “The frameworks that we’ve been using historically for privacy are no longer sufficient.” In his view the FTC will begin to consider not just whether companies caused monetary harm, but whether they violated consumers’ dignity because, for example, “There’s a huge dignity interest wrapped up in having somebody looking at your financial records when they have no business doing that.” See Stephanie Clifford, “Fresh Views at Agency Overseeing Online Ads,” New York Times, August 4, 2009.


190 Legal payment protections now differ depending on the type of payment product used (debit or credit) and the nature of the payment provider – traditional payment providers like Visa face legal requirements while new payment providers such as cell phone companies do not.

191 For example “Irish ISP Agrees to Three Strikes Against Its Customers” posted at the Electronic Freedom Foundation at http://www.eff.org/deeplinks/2009/01/irish-isp-agrees-three-strikes-against-its-users. Under the agreement the music labels, instead of going to court to get an order to have the ISP shut off a subscriber’s connection, provide evidence of infringement to the ISP directly. As the EFF commenter noted: “The difference is that an ISP is not a court; and its customers will never have a chance to defend themselves against the recording industry’s accusations and "proof". To whom, without judicial oversight, has the ISP obligated itself to provide meaningful due process and to ensure that the standard of proof has been met?”

192 Johnson and Post, p. 1389

193 Post in Jefferson’s Moose, pp. 178-186 describes “massively multi-player online games” or MMOGS as good candidates for this effort at online rule creation. I sympathize with his point that these new rule-making institutions will emerge only if people think that they are real. For this reason, a policy to defer in certain cases should be public and stable in order to provide the opportunity for the development of alternative rules.

194 Goldsmith and Wu p. 156.

195 Goldsmith and Wu p. 150.

196 See Johnson and Post at p. 1390: “One nation’s legal institutions should not monopolize rule-making for the entire Net.”

197 Goldsmith and Wu, p. 26

198 Goldsmith and Wu, p. 26

199 Goldsmith and Wu, p. 27. Reidenberg also argues that as jurisdictions increasingly conflict there will need to be an overarching harmonization of international rules. See Reidenberg States and the Internet at 230: “…online enforcement with electronic blockades and electronic sanctions will cause serious
international political conflicts. These conflicts arise because of the impact on territorial integrity. Such conflicts are likely to force negotiations toward international agreements that establish the legal criteria for a state to use technological enforcement mechanisms. This progression leads appropriately to political decisions that will define international legal rules.”

205 Goldsmith and Wu, p. 173
206 Goldsmith and Wu, pp. 152-160
207 Interestingly, the earlier Jack Goldsmith seemed more inclined to accept these practical considerations as a rationale for international harmonization: “When in particular contexts the arbitrariness and spillovers become too severe, a uniform international solution remains possible.” Goldsmith Against Cyber Anarchy p. 1235.

208 Berman p.1860
209 Berman p. 1860-1861


212 See presentation by Artemi Rallo Lombarte on International Standards On Data Protection & Privacy at https://www.agpd.es/portalweb/canaldocumentacion/comparecencias/common/IAPP_Privacy_Summit_09.pdf. He describes one of the main criteria of the global privacy standards project as “To elaborate a set of principles and rights aimed to achieve the maximum degree of international acceptance, ensuring at once a high level of protection.”